Aleksi Viitamäki

Aruba BYOD vai Citrix VDI suuryrityksen ratkaisuksi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

25.4.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Aleksi Viitamäki Aruba BYOD vai Citrix VDI suuryrityksen ratkaisuksi 53 sivua 25.4.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Service Production Vice President Pasi Ulkuniemi Yliopettaja Janne Salonen

Tässä insinöörityössä tutkittiin kahta markkinoilla olevaa vaihtoehtoa Bring Your Own Device -mallin käyttöönottamiseksi kansainvälisessä suuryrityksessä. Tutkitut tuotteet olivat pääsynhallintajärjestelmä Aruba ClearPass ja virtuaalityöpöytäratkaisu Citrix XenDesktop VDI. Tutkimuksen tavoitteina oli selvittää tuotteiden käyttöönoton helppoutta yrityksen IT:n näkökulmasta, käytettävyyttä käyttäjien näkökulmasta sekä tietoturvaa. Tutkimuksen kohteet valittiin niiden markkina-aseman ja tilaajayrityksen toiveiden mukaisesti.

Tutkimuksen aikana Aruba ClearPass rakennettiin aidosti ja testattiin käytännössä useilla eri laitteilla. Citrix XenDesktopin osalta käyttöönottoon Vmware-ympäristössä tutustuttiin dokumentaation avulla ja käytettävyyttä selvitettiin Internetin sekä haastattelun avulla. Työssä tutustuttiin myös BYOD:iin ja virtualisointiin yleisellä tasolla.

Tutkimuksen lopputulokseksi saatiin, että Aruba ClearPass edustaa tulevaisuuden kannalta parempaa ratkaisumallia. Omien laitteiden ja sovellusten lisääntyessä työntekijät haluavat lisääntyvissä määrin käyttää niitä myös työnteossa. Aruba ClearPass tarjoaa joustavan ja monipuolisen ratkaisun omien laitteiden pääsynhallintaan. Citrixin ratkaisu on varmatoiminen ja turvallinen, mutta pitkähkö asennusprosessi, ongelmat WAN-verkossa sekä tyypillisten toimisto-ohjelmien käytettävyys mobiililaitteilla rajoittaa sopivuutta kehitykseen pyrkivälle kansainväliselle yritykselle.

Insinöörityö on merkityksellinen tilaajayritykselle, koska tilaajan useat kansainväliset asiakkaat harkitsevat BYOD:in käyttöönottamista. Asiakkaat ovat toivoneet näkemystä, mikä on tulevaisuuden kannalta järkevin tapa edetä ottamalla huomioon käyttöönoton, tietoturvan ja aiemmat palvelut.

Avainsanat	BYOD, VDI, virtuaalityöpöytä, ClearPass, pääsynhallinta

Author(s) Title Number of Pages Date	Aleksi Viitamäki Aruba BYOD or Citrix VDI as Solution for Multinational Enterprise 53 pages 25 April 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networks
Instructor(s)	Pasi Ulkuniemi, Service Production Vice President Janne Salonen, Principal Lecturer

This thesis investigated two on-market solutions for introducing Bring Your Own Device to a multinational enterprise. The investigated solutions were Aruba ClearPass access control system and the desktop virtualization system Citrix XenDesktop VDI. The goals were to find out how easy the solutions are to implement from the IT point of view, how usable the solutions are from the user's point of view how secure the solutions are. These solutions were selected because of their market status and also because the commissioner of this study requested it.

During the study Aruba's ClearPass solution was built to a lab environment and tested with multiple mobile platforms. Citrix XenDesktop Vmware implementation was studied from a deployment guide and its usability reviews were gathered from the Internet and in an interview. The study also gives information about BYOD and desktop virtualization in general.

The study indicates that Aruba ClearPass represents long lasting solution which aims to the future. As smart device markets keep growing, more employees want to use their own devices and software. ClearPass offers a flexible solution for controlling the access of these devices. Citrix's solution is stable and safe but the long implementation process, issues with WAN connections and low usability of typical office software with smart devices makes Citrix a less preferred choice for developing multinational enterprise.

This thesis is important to the commissioner as its global customers have requested best practice information regarding the implementation of BYOD.

Keywords	BYOD, VDI, virtual desktop, ClearPass, access control

Sisällys

Lyhenteet

AD	Active Directory. Microsoftin palvelinohjelmisto, jonne talletetaan mm. käyttäjät ja ryhmät.
BYOD	Bring Your Own Device. Yleiskäsite, jolla kuvataan oman laitteen käyttöä esimerkiksi työpaikan verkossa.
CMS	Content Management System. Julkaisujärjestelmä, usein sivusto, jonka sisältöä käyttäjät voivat muokata, lisätä ja poistaa.
DHCP	Dynamic Host Control Protocol. Jakaa IP-osoitteita verkkoon liittyville laitteille.
EDGE	Enhanced Data rates for GSM Evolution. Alias 2,75G. Matkapuhelinten tiedonsiirtotekniikka.
GPRS	General Packet Radio Service. Alias 2,5G (Generation). Matkapuhelinten tiedonsiirtotekniikka.
HSPA	High-Speed Packet Access. Alias 3G. Matkaviestinteknologia.
IEEE 802.1x	Institute of Electrical and Electronic Engineersin määrittelemä standardi porttikohtaisesta todentamisesta.
IP-osoite	Internet Protocol -osoite. Verkkoon liitetyn laitteen osoite.
LTE	Long Term Evolution. Alias 4G. Uusin kaupallinen matkaviestinteknologia.
MAC	Media Access Control. Verkkokortin yksilöllinen osoite.
MDAC	Mobile Device Access Control. ClearPassin edeltäjä.
MDM	Mobile Device Management. Järjestelmä, jolla voidaan hallinnoida mobiililaitteita verkossa.
MOVE	Mobile Virtual Enterprise Architecture. Aruban BYOD-arkkitehtuuri.

OPEX	Operating Expense. Käyttökustannus.
OTA	Over The Air Programming. Tapa tuoda esim. päivityksiä laitteisiin.
OUI	Organizationally Unique Identifier. MAC-osoitteen alkuosa, joka usein määrittää valmistajan.
RADIUS	Remote Authentication Dial In User Service. RFC 2868 -määrittely.
SaaS	Software as a Service. Ohjelmisto, joka hankitaan palveluna lisensoinnin sijasta.
SAN	Storage Area Network. Arkkitehtuuri tiedostopalvelimien yhdistämiseksi.
SNMP	Simple Network Management Protocol. Protokolla, jolla voidaan hallita ja tehdä kyselyitä verkkolaitteille.
SQL	Structured Query Language. Kyselykieli, jolla voi tehdä erilaisia käskyjä relaatiotietokantoihin.
TCO	Total Cost of Ownership. Laskennallinen omistuskulu.
VDI	Virtual Desktop Infrastructure. Teknologia, jolla työpöydän tuodaan laitteeseen siten, että itse työpöytä ei ole asennettu laitteelle vaan palvelimelle konesalissa.
VLAN	Virtual Local Area Network. Pakettiliikenteen tägityksellä toimiva teknologia, jolla fyysisesti samassa sijainnissa olevia käyttäjiä voidaan sijoittaa eri verkkoihin.
VPN	Virtual Private Network. Teknologia, jolla kaksi verkkoa voidaan yhdistää tietoturvallisesti julkisen verkon yli. Perustuu tunnelointiin.
WAN	Wide Area Network. Verkkoja, jotka käsittävät suuria maantieteellisiä alueita.
WLAN	Wireless Local Area Network. Langaton lähiverkko.

1 Johdanto

Tässä insinöörityössä pyritään vertailemaan kahta markkinoilla olevaa ratkaisua Bring Your Own Device -ratkaisuna kuvitteellisessa kansainvälisessä suuryrityksessä. Yrityksen työntekijöiden ajatellaan olevan paljon matkustavia ja melko vapaita työnsä tekemisessä. He saattavat työskennellä toimistolla työpisteellään, neuvotteluhuoneessa ja oleskelutiloissa sekä kotonaan, asiakkaiden luona sekä oman yrityksen sivukonttoreissa ympäri maailman. Työntekijät haluavat käyttää työssään yhä enemmän tabletteja, älypuhelimia ja kannettavia tietokoneita yrityksen tarjoaman kannettavan tietokoneen sijaan.

Vertailua tehdään WLAN-valmistaja Aruban ClearPass-tuotteen ja ohjelmistotalo Citrixin XenDesktopin Dedicated VDI -tuotteen kesken. Näistä ensimmäistä pidetään tässä työssä niin sanottuna aitona BYOD:na, koska sillä voidaan sallia käytettävälle laitteelle pääsy suoraan yrityksen verkkoon. VDI-ratkaisussa pääsy sallitaan käyttämällä laitteelle asennettavaa erillistä ohjelmaa, jolla käyttäjä pääsee käyttämään muualla, tässä tapauksessa konesalissa, ajettavaa työpöytää. Tämän vuoksi tässä työssä VDI:stä ei puhuta BYOD:na, vaikka siitä sen kaltaisia piirteitä löytyykin. VDI:tä usein myös markkinoidaan BYOD:na.

Työn tavoite on tutkia mainittujen kahden valmistajan tuotteiden käytettävyyttä, käyttöönoton helppoutta ja tietoturvaa. Työn rajaamiseksi vain Aruban ympäristö rakennetaan aidosti tutkimuksen aikana. Citrixin osalta tutkimus tehdään dokumentaation, Internet-lähteiden ja haastattelujen pohjalta. Työssä ei oteta kantaa muihin markkinoilta löytyviin vastaaviin ratkaisuihin. Lähtökohtana ja väittämänä tutkimukselle on, että Aruban ratkaisu on tutkittavan kohteen, kansainvälisen suuryrityksen tarpeisiin parempi niin käyttöönoton kuin käytettävyytensä osalta.

Työ tehdään Forte Netservices Oy:lle, joka pyysi tutkimaan BYOD:ia myyntiviestin ja tuotekehityksen tarpeisiin. Forte toivoo parempaa ymmärrystä, miten nykyisin käytössä olevat päätelaitteet tukevat yritysten sovellusten käyttämistä, jotta voidaan varmistua, ettei kyseessä ole vain uusi markkinointihype.

2 Bring Your Own Device

2.1 Historia

Bring Your Own Device on tällä hetkellä yksi puhutuimmista uusista innovaatioista. Älypuhelinmarkkinat ovat kasvaneet räjähdysmäisesti Applen julkistettua iPhonen vuonna 2007. Applen kilpailijoiden Googlen Androidin ja Microsoftin Windows Mobilen myötä jopa 70 % vuonna 2012 myydyistä mobiililaitteista oli älypuhelimia tai tabletteja. Gartnerin ennusteen mukaan vuoteen 2016 mennessä kaksi kolmasosaa maailman liikkuvasta työvoimasta käyttää niin kutsuttua älylaitetta. Trendin voimakkuutta kuvaa esimerkiksi tietoturvalaitteisiin erikoistuneen valmistaja Fortinetin vuonna 2012 teettämä kysely, jonka mukaan kaksi kolmasosaa yritysten nuorista työntekijöistä pitää oikeutenaan tuoda töihin omia laitteitaan ja käyttää niitä työnteossa. [1; 2; 3.]

BYOD:in historia juontuu jopa yli kymmenen vuoden päähän, kun yliopistot alkoivat muuttaa omaa tietoturvapolitiikkansa siten, että opiskelijat ja työntekijät voisivat käyttää omia laitteitaan koulun verkossa. Käytännössä tämä tarkoitti usein avointa tai jaetulla avaimella salattua langatonta verkkoa, johon pääsi yhdistämään laitteesta riippumatta kunhan oli vain saanut ohjeet. Opiskelijat tai työntekijät saivat yhdistämisen jälkeen hieman riippuen erilaisia pääsyoikeuksia sisäverkkoon ja Internetiin. Verkkosivukehityksen ja erityisesti CMS-julkaisujärjestelmien kehittymisen myötä BYOD voitiin laajentaa siten, että järjestelmiä pystyi käyttämään jopa kotoa asti.

2000-luvun alussa WLAN oli teknologiana vielä verrattaen kehittymätön. Ensimmäisestä GSM-puhelustakaan ei ollut aikaa kuin vasta kymmenen vuotta, ja langattomia verkkotuotteita oli markkinoilla melko vähän. Vuosituhannen vaihteen jälkeen kaikki kuitenkin muuttui: Ensin IEEE julkaisi vuonna 2003 WLAN:in g-standardin 802.11g ja sitten vuonna 2009 huomattavasti kehittyneemmän n-standardin. G-standardin tavoin n-standardi sai erittäin suuren suosion ja on yleisesti käytössä ympäri maailman. Samaan aikaan teleoperaattorien mobiiliverkot kehittyivät ja jo 1990-luvun puolella kehitetty GPRS (2,5G) kehittyi EDGE:ksi (2,75G) vuonna 2003 ja tästä edelleen HSPA:n (3G) ja sen eri kehitysasteiden kautta nykyään yleistymään päin olevaan, vuonna 2009 kaupallistettuun LTE-standardiin (4G). Tämä tarkoitti mobiilikäyttäjille suurta mullistusta: enää ei tarvinnut olla modeemia ja johtoa Internetiin yhdistämiseksi, vaan esimerkiksi puhelin tai kannettava tietokone riitti. Nokia lanseerasi vuonna 2004 oman 9500-kommunikaattorinsa, jota voidaan pitää yhtenä ensimmäisistä

varteenotettavista älypuhelimista lähinnä Symbian-käyttöjärjestelmän ja WLAN ominaisuuksien vuoksi. Aluksi markkinat kasvoivat hitaasti, mutta Symbianin kehittyessä yrityksiä alkoi kiinnostaa esimerkiksi sähköpostin tuominen puhelimiin. Vaikeutena oli kuitenkin edelleen puhelimien pienet näytöt, hitaus ja hankalat käyttöliittymät. IT-yksiköille ongelmia tuotti Symbianin integroiminen yrityksen verkkoon, johon ei pitkään aikaan ollut mitään toimivia ratkaisuja ja lähes aina käyttäjän piti tuoda puhelimensa IT:lle, jotta edes sähköpostit saatiin puhelimeen. [4; 5; 6; 7; 8.]

Vuonna 2007 Yhdysvaltalainen Apple mullisti maailman tuomalla markkinoille iPhonen. Se ei suinkaan ollut ensimmäinen kosketusnäytöllinen puhelin, mutta sen innovatiivinen käyttöjärjestelmä iOS oli markkinoilla aivan uutta. Suuren kosketusnäytön ja helppokäyttöisen käyttöjärjestelmän myötä se houkutteli asiakkaikseen kaikkien perinteisten mobiilivalmistajien asiakkaita. Apple sai nopeasti myös kilpailijoita: muun muassa Googlen Androidin ja Microsoftin Windows Mobilen. Erityisesti Android kasvatti räjähdysmäisesti markkinaosuutensa yli puoleen koko älypuhelinmarkkinoista. Samaan aikaan Apple kehitti iPadin, tablettitietokoneen, joka sai nopeasti kilpailijansa Androidia käyttävistä valmistajista. Vuoden 2007 julkistuksesta lähtien yhä useammalta löytyy helppokäyttöinen ja erittäin monipuolinen älylaite taskustaan. Yritysmaailmassa alkoi esiintyä yhä enemmän omia laitteita, omia sovelluksia ja omalaatuisia tarpeita. BYOD:in tarve kasvoi merkittävästi. [9; 10.]

BYOD-termin tarkkaa ensimmäistä käyttökertaa ei tiedetä, mutta termi syntyi vuoden 2011 tietämillä, kun yrityksissä havaittiin, että jopa puolella työntekijöistä on oma älypuhelin, tabletti tai kannettava tietokone, jota työntekijät halusivat käyttää työssään. Samoihin aikoihin syntyi myös BYOD:in verrattavia termejä: BYOT (Technology), BYOP (Phone), BYOPC (PC, Personal Computer). Taustalla on toinen trendiksi noussut termi kuluttajaistuminen, englanniksi consumerization. Yrityksissä tilanne nähdään sekä työtehoa parantavana että yritykselle taloudellisesti kannattavana asiana. BYOD:in eräs etu on se, että yrityksen IT-yksikkö voi määritellä tietynlaiset säännöt jo etukäteen, ja kun käyttäjä lopulta tuo oman laitteensa verkkoon, hän pystyy itse rekisteröimään laitteensa eikä IT:n osallistumista enää siinä vaiheessa tarvita. BYOD:in yleistymistä ovat hidastaneet erilaiset pelot muun muassa tietoturvasta, kontrollin menettämisestä, kirjavan laitekannan hallittavuudesta sekä puhdas konservatiivinen ajattelu siitä, että yrityksen tulee omistaa kaikki verkossa olevat laitteet. Lisäksi markkinoilla on ollut melko vähän toimivia ratkaisuja BYOD:in toteuttamiseksi yritysverkossa. [8; 11.]

Kuva 1. BYOD:in perusajatus. Kuvan lähde: Aruba Networks.

Kaikesta huolimatta BYOD on terminä suorastaan nykyhetken hype ja yleistynyt merkittävästi markkinoille saatujen työkalujen myötä. Jo syksyllä 2011 tehdyssä tutkimuksessa (Current Analysis: BYOD and MDM trends) 80 % yli 500 työntekijän amerikkalais- ja eurooppalaisyrityksistä ilmoitti käyttävänsä BYOD:ia jossakin muodossa omassa verkossaan. Pääasiassa kyse oli tällöin hyvin kontrolloidusta VPN-ympäristöstä, eikä niinkään omien laitteiden käyttämisestä jokapäiväisessä työssä yrityksen omien laitteiden tavoin. Myös mobiililaitteiden, kuten älypuhelinten ja tablettien pääsy yritysten verkkoon oli vähäistä puhumattakaan oman laitteen kytkemisestä johdolla yrityksen verkkoon. Tulevaisuudessa BYOD:n uskotaan yleistyvän merkittävästi toimivien hallintatyökalujen ja asenteiden muuttumisen myötä. Muun muassa Aruba povaa vuodelle 2013 suurta kasvua ClearPassin osalta. ClearPassin yhtenä vahvuutena onkin, että sama laite voidaan sallia verkkoon niin verkkokaapelia pitkin kuin langattomastikin. Asiaan palataan luvussa 2.4 tarkemmin. [8; 9; 10; 11; 12; 13; 14.]

2.2 BYOD-hallintamallit

2.2.1 Keskitetty

BYOD:in keskitetyn hallintamallin perusajatus on yksinkertainen. Mallissa yritys keskeisesti hallinnoi BYOD:ia verkossaan. Hallintaa voi olla yksi tai useampi seuraavista piirteistä:

- Yritys valvoo BYOD-palveluita keskitetysti esimerkiksi hallintasovelluksen, kuten ClearPassin avulla.
- Yritys vaatii käyttäjiltä pääsyoikeudet verkkoon yhdistettävään laitteeseen, jotta se voidaan esimerkiksi varkaustilanteessa tyhjentää etänä. Verkossa ajetaan siis MDM (Mobile Device Management) -järjestelmää, esimerkiksi Microsoft Exchange ActiveSynciä.
- Yritys vaatii tietoturvapolitiikassaan, että yhdistettävä BYOD-laite täyttää tietyt vaatimukset esimerkiksi käyttöjärjestelmän, virustorjunnan, laitevalmistajan tms. osalta.
- Verkkoon tunnistaudutaan henkilökohtaisilla käyttäjätunnuksilla. Käytössä voi olla kaksivaiheinen tunnistautuminen.
- Käyttöönottoon tarvitaan IT-tuen toimenpiteitä.
- Yritys vaatii käyttäjät valitsemaan oman laitteensa yrityksen laitetarjottimelta tai tarjoaa tietyn rahasumman laitteen hankkimiseen. Yritys ostaa ja omistaa laitteet, mutta välttämättä laitteiden sovelluksiin, sisältöön tai käyttöön ei muuten puututa.

Viimeisintä kohtaa kutsutaan myös CYOD:ksi, Choose Your Own Device, valitse oma laitteesi. Sen uskotaan olevan yritysmaailmassa alkusysäys varsinaiseen BYOD:in siirtymiseen, koska tällöin yritykset pääsevät hallitusti rakentamaan BYOD ympäristöään. Keskitetty malli tulee todennäköisesti olemaan ylivoimaisesti yleisin BYOD:in malli, koska yritysmaailmassa avoin ja kontrolloimaton ympäristö on IT:n kannalta turvaton ja jopa vaarallinen. [15; 16; 17.]

2.2.2 Avoin

Avoin BYOD:in hallintamalli on käytännössä keskitetyn hallintamallin vastakohta. Siinä voi olla piirteitä keskitetystä mallista, kuten rajauksia verkoon pääsyn osalta. Oleellista on, että avoin malli on hyvin liberaali. Avoimen mallin piirteisiin kuuluu:

- Verkko, johon pääsee millä tahansa laitteella.
- Salasanoja ei ole, tai ne voivat olla jaettuja kaikkien käyttäjien kesken.
- Pääsyrajoituksia verkon sisällä ei ole.
- Sisäverkkoa ei ole, vaan verkosta pääsee ainoastaan suoraan Internetiin.
- Käyttöönotto on vaivatonta eikä vaadi IT-tuelta toimenpiteitä.

Avoin malli voi olla käytössä esimerkiksi julkisilla paikoilla, kuten esimerkiksi julkisissa kulkuvälineissä, lentokentillä ja kahviloissa. Mallia käytetään myös yleisesti yliopistoilla, kotona ja yritysten vierailijaverkoissa. Avoin malli helpottaa huomattavasti verkon käyttöä käyttäjän näkökulmasta. BYOD:iin liitetään myös käyttöönoton helppous, jossa IT-tuen toimenpiteitä ei tarvita. Avoin malli pitää kuitenkin sisällään piirteitä, jotka jättävät verkon ja muut sen käyttäjät hyvin alttiiksi monille erilaisille riskeille mukaan lukien tietoturva- ja haittaohjelmaongelmat. Tarvittaessa avoimenkin verkon liikennettä voidaan skannata esimerkiksi ennen Internetiin pääsyä, mikä vähentää haittaohjelma- ja hyökkäysriskiä verkossa merkittävästi. Avoimen mallin ei silti uskota yleistyvän yritysympäristöissä juuri lainkaan.

2.2.3 Hajautettu

Hajautetussa hallintamallissa on poimittu ideoita sekä keskitetystä että avoimesta hallintamallista. Esimerkiksi suuryrityksen näkökulmasta työntekijöiden BYOD saattaa olla hyvinkin keskitetty, kun taas vierailijat päästetään verkkoon avoimen mallin mukaisesti. Vierailijatkin saatetaan yhdistää esimerkiksi Aruban ClearPassin kaltaisen järjestelmän läpi, joka taustalla analysoi verkkoon liitettyä laitetta ja sen liikennöintiä verkossa. Aruban tuote tämänkaltaiselle toiminnallisuudelle on nimeltään ClearPass Guest. Tarvittaessa järjestelmä tunnistaa rikkeen ja poistaa laitteen verkosta. Samaan aikaan verkossa voidaan ajaa ClearPass OnBoardia, joka rakennetaan tässä työssä luvussa 4. OnBoard antaa yrityksen IT-tuelle mahdollisuuden vähentää työmääräänsä ja antaa käyttäjien rekisteröidä itse omat laitteensa verkkoon ilman IT-tuen osallistumista.

2.3 BYOD:in hyödyt ja haitat

2.3.1 Hyödyt

Erilaisten jo aiemmin mainittujenkin tutkimusten pohjalta on päädytty usein samanlaisiin tuloksiin: työntekijät ja erityisesti nuoret haluavat käyttää omia laitteitaan ja ohjelmistojaan. Laite- ja ohjelmistovapauden vuoksi BYOD:in katsotaan parantavan merkittävästi työssä viihtymistä. Useat nimenomaisesti älylaitteille suunnitellut sovellukset, kuten Skype, Dropbox, Facetime, Lync, GoToMeeting ja vastaavat pilvipalvelut helpottavat työntekoa sekä tiedon jakamista. Perinteiset asiakas-palvelin-sovellukset ovat jäämässä ajasta ja kehityksestä jälkeen uusien teknologioiden ja alustojen kehittyessä huimaa vauhtia ympärillä. Työntekijät ajattelevat, että omia laitteita on miellyttävä käyttää ja ne tunnetaan paremmin. Usein vikatilanteessa käyttäjä saattaa pystyä ratkaisemaan helpommin omaan laitteeseensa liittyvän ongelman. Oman laitteen haaste voi olla myös motivaattori: ei suostuta ottamaan yhteyttä yrityksen IT-tukeen vaan ongelma ratkaistaan itse. Työssä viihtyvyys ja omat työkalut ovat myös tehokkuuteen liittyviä asioita. Töitä pystytään tekemään nopeammin omilla laitteilla ja omalla tyylillä. Oman langattoman tabletin kanssa voi työskennellä toisenlaisessa ympäristössä, kuin avokonttorin sermien sisällä. Tabletti on helppo ottaa palaveriin mukaan, koska sitä voi tarvittaessa käyttää myös paperimuistion korvikkeena. Samalla palaveriin osallistujat eivät piiloudu kannettavien näyttöjen taakse vaan pystyvät tehokkaammin osallistumaan palaverissa käytäviin asioihin. Työssä viihtyvyys puolestaan on tärkeä työskentelymotivaatioon, ja sitä kautta yrityksen tulosta parantava seikka. Omia laitteita käyttämällä IT ei useimmiten ole enää niin ongelmallista. [8.]

BYOD:ia pidetään lähtökohtaisesti yritykselle taloudellisesti kannattavana ratkaisuna. Investointina BYOD-järjestelmä ei tuo säästöjä, mutta säästöjä syntyy, kun työntekijät tuovat omat laitteensa ja yrityksen ei tarvitse tehdä erikseen laitehankintoja. Joissain maissa, kuten esimerkiksi Yhdysvalloissa puhelinliittymiä ei käytännössä voi ostaa ilman kytkypuhelinta. Perinteinen IT:n tapa hankkia laitteet erikseen ja postittaa ne vastaanottajille on tässä mielessä kaksinkertainen kustannus, kun käyttäjät kuitenkin saavat kytkykaupasta liittymän mukana puhelimenkin, josta yritys kuitenkin koko ajan maksaa kuukausimaksuissa. Säästöjä saadaan myös IT-tuen tarpeen vähenemisen kautta. Yrityksen kannalta parhaassa tapauksessa yritys voi jopa lopettaa oman IT:n tuottamisen ja ulkoistaa palveluntuottajalle yrityksen toiminnan kannalta kriittiset palvelut, kuten palvelimet ja BYOD-järjestelmän. Säästää voi myös puhelinkuluissa,

kun työntekijät käyttävät omia liittymiään. Oletettavaa kuitenkin on, ettei ainakaan Suomessa puhelinkulujen siirtäminen työntekijöille tule yleistymään. [8.]

Teknologian uutuus viehättää monia. BYOD on yritysmaailman näkökulmasta uusi teknologia, joka nähdään haasteena mutta samalla etuna. Osassa suuryrityksiä BYOD:n käyttöön kannustetaan jo nyt, ja teknologian kysyntä on kasvanut jatkuvasti. Viime vuosina on ollut lukuisia esimerkkejä erittäin onnistuneista uusista teknologioista, kuten esimerkiksi kosketusnäytöt, HSPA-verkot ja Android-mobiilialusta. Näiden kaltaiset onnistumiset rohkaisevat yrityksiä kokeilemaan uusia vaihtoehtoja tehostamaan yrityksen toimintaa. [8.]

BYOD voi myös parantaa yrityksen tietoturvaa erityisellä keinolla. Laite- ja ohjelmistokirjon ollessa laaja yritykseen on vaikea kohdistaa laajaa vaikutusta aiheuttavaa suunniteltua hyökkäystä. Mikäli pääjärjestelmät, kuten palvelimet on suojattu riittävällä tavalla, on nykyaikana tavallisesti nähtäviä tiettyyn yritykseen kohdistettuja hyökkäyksiä vaikeampaa toteuttaa. BYOD-verkon voi suojata hyvinkin perinteisillä ja toimivilla teknologioilla, kuten RADIUS-autentikoinnilla ja tässäkin työssä esiteltävällä ClearPass-pääsynrajausjärjestelmällä.

2.3.2 Haitat

BYOD:in vastustajat osaavat luetella lukuisia kriittisiä ongelmia omien laitteiden sallimisessa verkkoon. Lähes poikkeuksetta BYOD:n vastustus tuleekin yrityksien IT-yksiköistä, joissa pelätään muun muassa kontrollin menettämistä ja adhoc-tuen siirtymistä yrityksen IT:n vastuulle. [8.]

Siinä missä BYOD voi olla taloudellisesti yritykselle kannattava laitehankintojen vähenemisen vuoksi, voi se myös olla ainakin alkuun taloudellisesti kannattamaton monin tavoin. Ensisijaisesti BYOD vaatii investointeja itse järjestelmään, mutta myös yrityksen verkkoon. Vanha laitekanta harvoin tukee BYOD:n asettamia vaatimuksia autentikoitumisen ja datamäärien suhteen, jolloin edessä saattaa olla suurempi verkon päivitysprosessi. Myös BYOD:ssa on omat lisensointikustannuksensa, usein käyttäjä tai laitepohjaisesti, jotka tällä hetkellä kasvavat joka vuosi. BYOD:in mukanaan tuoma laitekirjo saa nopeasti IT-yksikön suurten haasteiden eteen, kun järjestelmiä ja laitekokoonpanoja on yhtä paljon kuin käyttäjiäkin. Työaikaa voi mennä monesta näkökulmasta hukkaan, kun erikoisia ongelmia selvitellään käyttäjien kanssa.

Laitehankintojen lisäksi laitteiden varkauksien tai katoamisten varalle tarvitaan ainakin MDM, kuten esimerkiksi ActiveSync. Myös Aruba julkaisi tutkimuksen aikana ClearPassin MDM-lisäosan Workspacen, mutta sitä ei ehditty ottaa tutkimukseen mukaan. Yleisesti markkinoilla olevat MDM- ja BYOD-ratkaisut saattavat olla hyvinkin kalliita. Suuryrityksessä hankintojen määrä on kuitenkin vähäisempi kuin käyttäjille omia laitteita hankittaessa. [8; 9, sivu 2; 17; 18.]

Teknologian uutuus on yksi BYOD:in haasteita, vaikka se on myös hyöty. Kokonaisvaltaisia ja toimivia BYOD-järjestelmiä on markkinoilla vasta vähän. MDM-järjestelmiä on tarjolla useita, mutta niiden ominaisuudet eivät välttämättä riitä yrityksille. Suurin osa järjestelmistä ei tue kuin muutamaa alustaa tai vain tiettyjä valmistajia. Isoimpia ongelmia kuitenkin lienee se, että yrityksen sovellusten käyttö on edelleen haastavaa omilla laitteilla. Asiakas-palvelin-sovellukset on alunperin suunniteltu perinteiseen yritysverkkoon eikä BYOD-ympäristöön tai kosketusnäytöllä käytettäväksi. Esimerkiksi Word-dokumentin lukeminen voi vielä onnistua kosketusnäyttölaitteella, mutta muokkaus on hankalaa. Lisensointiongelmat ja alustojen epäsopivuudet aiheuttavat sen, ettei kaikkia tarvittavia sovelluksia edes saada asennettua omiin laitteisiin. Tähän mennessä parhaiten ovatkin yleistyneet erilaiset selainpohjaiset ohjelmistot, joita voidaan käyttää lähes laitteella kuin laitteella, kunhan siinä on www-selain. Myös täysin pilvipalveluina olevat sovellukset (SaaS) ovat yleistyneet merkittävästi. [8.]

Tietoturvahaasteet ovat tällä hetkellä BYOD:in puhutuimpia ongelmia. BYOD-järjestelmien tietoturvaa arvostellaan heikoksi ja niiden arvioidaan vaarantavan yrityssalaisuudet, jotka tallentuvat käyttäjän omaan laitteeseen. Yritys joutuu puntaroimaan, miten tieto salataan erityisesti kannettavilla tietokoneilla, jotka tallettavat paljon tietoa omaan muistiinsa, ja mitä tehdä, kun työntekijän työsuhde päättyy. Pahimmassa tapauksessa vuotava tai varastettu työntekijän BYOD-laite saattaa aiheuttaa yritykselle mittavaa taloudellista vahinkoa, esimerkiksi viruksen lamauttaessa tärkeitä järjestelmiä, ja antaa kolauksen yrityksen maineelle. BYOD voi myös altistaa yrityksen pitkäaikaiseen vakoiluun tai häirintään, jossa sivullisena kärsijänä voi olla vuotavan laitteen omistava työntekijä. [8.]

BYOD:in valintaa harkitessaan yrityksen täytyy punnita tarkoin siinä nähtävät hyödyt ja haitat. Hyötyjä ei kannata vähätellä, koska BYOD:n toimiessa yrityksen toimintateho voi parantua merkittävästi. Edellä mainittujen riskien ei pitäisi antaa lannistaa tietoverkon kehittäjiä. Tässä työssä pyritään todistamaan, että BYOD:iin voidaan siirtyä

askeleittain, eikä BYOD:ia tarvitse ottaa alusta alkaen koko laajuudessaan käyttöön. Työssä lisäksi pyritään todistamaan, että BYOD:in käyttöönotto Aruban ClearPassia käyttäen on IT-yksikölle vaivatonta ja yrityksen verkon näkökulmasta turvallista.

2.4 Aruba ClearPass

Aruba esitteli vuonna 2011 MOVE™-arkkitehtuurinsa. Taustalla oli idea ”LAN Is Dead – Lähiverkko on kuollut”. Tällä viitattiin luonnollisesti perinteiseen lähiverkkoon, jossa oli tarkasti rajatut VLANit, 802.1x-autentikointi RADIUS-palvelimelta ja yritysverkkoon pääsi vain yrityksen omilla laitteilla. Aruban tavoitteena oli houkutella yrityksiä BYOD-trendiin mukaan tarjoamalla MDAC-alusta Applen iOS-laitteille. Vuonna 2011 Aruba osti ensin Amigopodin, joka oli tuottanut ohjelmistoa, jolla voidaan itse rekisteröidä laite verkkoon. Myöhemmin samana vuonna Aruba hankki Avendan, joka oli tuottanut eTIPS-ohjelmistoa, jolla pystyttiin profiloimaan ja tutkimaan verkkoon liitettävä laite automaattisesti ja antamaan sille oikeudet tiettyjen sääntöjen perusteella. Näiden hankintojen tuloksena vuonna 2012 MOVE sai täydennystä ClearPass-tuoteperheestä. Jälleen taustalla oli osuva slogan ”People Move. Networks Must Follow – Ihmiset liikkuvat. Verkkojen täytyy seurata”. ClearPass vei Aruban MDAC:ia kehityksessä eteenpäin. Se pitää sisällään tuen tunnetuimmille käyttöjärjestelmille, Android ja Windows mukaan lukien, ja tarjoaa selkeät, erikseen ostettavat komponentit, jotka yritys voi valita tarpeidensa mukaan. Komponentit ovat ohjelmia, joita ajetaan ClearPass Policy Managerin päällä. [19; 20; 21.]

2.4.1 MOVE-arkkitehtuuri

Nykyinen tietoverkko ei enää riitä yrityksille. Tämä on koko Aruban MOVE-arkkitehtuurin lähtökohtana. Työntekijät matkustavat paljon, ja he käyttävät työssään samanaikaisesti monenlaisia eri laitteita sekä eri tapoja yhdistää verkkoon: WLAN, langallinen yhteys, 3G-verkko, VPN ja niin edelleen. Tästä syystä yrityksillä on jo nyt haaste. Vanhan suunnittelutavan mukaiset VLANit eivät välttämättä riitä kokonsa puolesta tai skaalaudu verkon kasvulle. Erilaiset sovellukset, kuten YouTube, videoneuvottelut, etätyöpöydät ja -ohjelmat vaativat suurempaa kaistanleveyttä ja laatua (QoS). Koska työntekijät yhdistävät verkkoon lukuisilla eri laitteilla, ei tietoturvaa pystytä enää rajoittamaan järkevästi ja tehokkaasti. Yrityksillä saattaa olla käytössään lukuisia osittain päällekkäisiä valvonta- ja pääsynhallintajärjestelmiä: omansa langalliselle verkolle, omansa langattomalle, omansa VPN:lle, jne. Ongelma paisuu

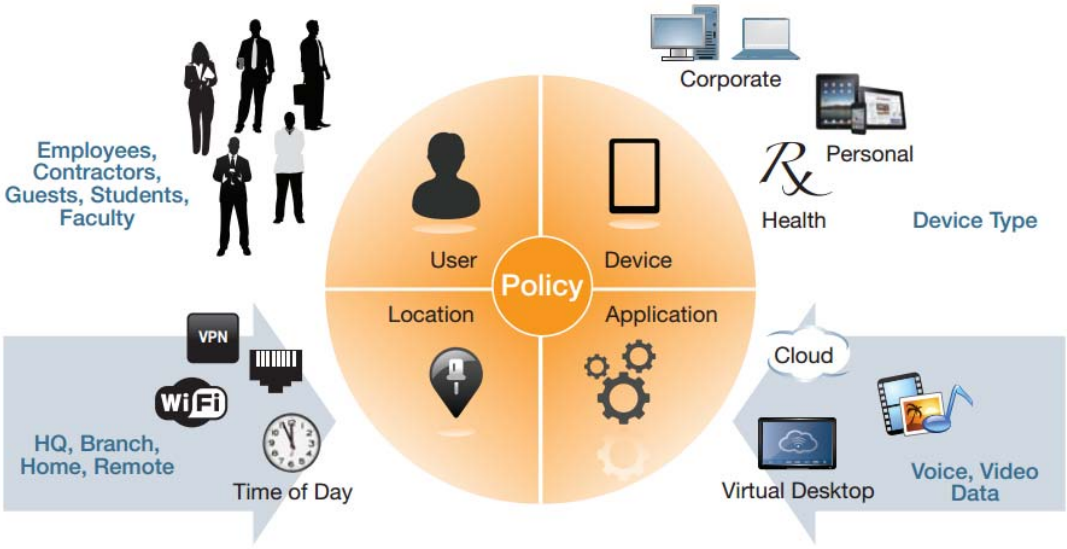
vielä entisestään, jos näiden järjestelmien hallinnoinnista vastaavat eri henkilöt. [19; 22.]

Kun yrityksen verkkoon lisätään esimerkiksi uusi sovellus, joka tarvitsee pääsyn tiettyihin resursseihin (esimerkiksi palvelimille), ja vastaavasti työntekijät tarvitsevat pääsyn uuteen sovellukseen, tulee ongelma parhaiten esiin. Pyynnöt tarvittavan liikenteen avaamisesta saatetaan lähettää usealle eri taholle. Lopputuloksena VPN:n kautta saattavat olla kaikki protokollat ja kohdeosoitteet sallittuna, kun taas lankaverkosta hyvin rajatusti vain tietyt portit ja resurssit. Langattomasta verkosta ei välttämättä ole pääsyä ollenkaan. Työntekijälle tilanne näkyy takkuavana IT:nä. Jokin päivä sovellus toimii, toinen päivä ei. Saattaa mennä pitkä aika, ennen kuin IT tai työntekijä löytää aidon syy-seuraussuhteen, eritoten jos työntekijä käyttää toimistolla ollessaan välillä WLANia ja välillä lankayhteyttä. Todellisuudessa syy on siinä, että verkon hallinta on hajautettu ja jokaisen eri osa-alueen hallinnoija on todennut pääsyn tarpeen eri tavalla. [19; 22.]

Toinen ongelma ilmenee, kun yrityksen sivutoimistolla osallistutaan tärkeään videoneuvotteluun. Maantieteellisistä tai taloudellisista syistä johtuen sivutoimiston koko Internet-kapasiteetti on 5 Mbps. Videoneuvottelusta täysin tietämätön saman konttorin työntekijä viettää ruokataukoaan katsellen YouTube-videoita. Samaan aikaan neuvotteluhuoneessa video ja ääni katkeilee eikä neuvotteluun kyetä osallistumaan täysipainoisesti. [19; 22.]

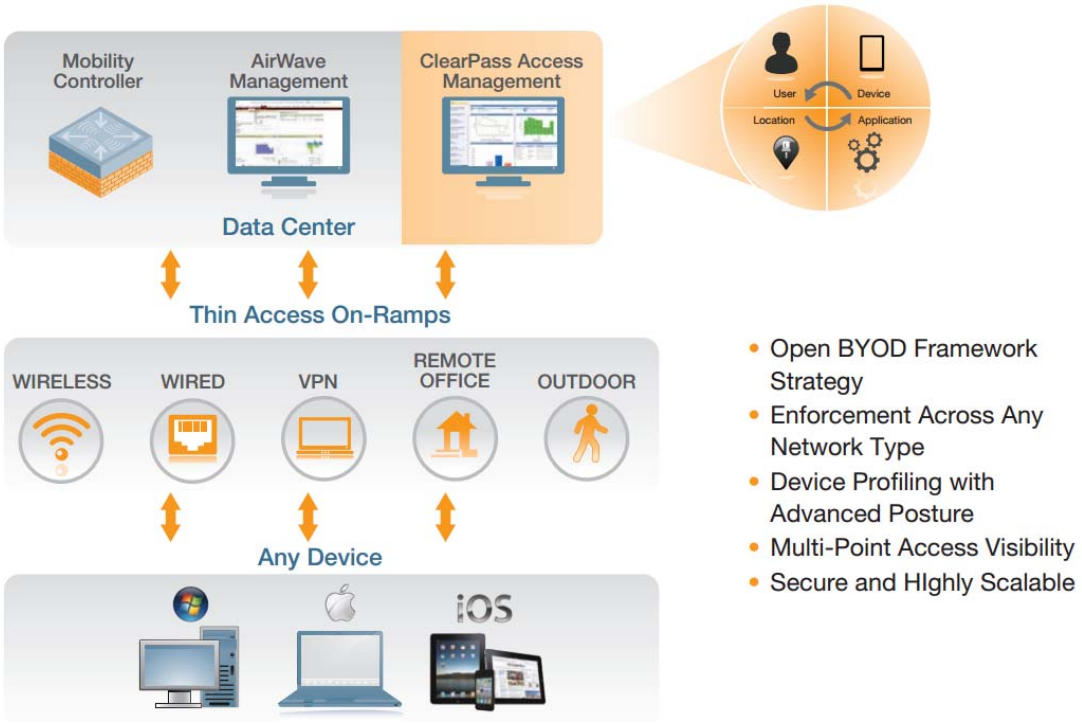
Aruban ratkaisu on MOVE-arkkitehtuuri. Se perustuu pohjimmiltaan neljään perusajatukseen:

- VLANit ovat vanhentuneita eikä niille ole käyttöä nykyverkossa.
- Verkon pitää olla teknologioiden (WLAN, ethernet, 3G, VPN) osalta yhdistävä tai sama.
- Laite- ja käyttäjähallinnan tulee olla keskitetty yhteen paikkaan sijainnista tai yhdistämistavasta riippumatta.
- Sovellukset täytyy kyetä tunnistamaan, jotta tärkeille sovelluksille voidaan antaa riittävä prioriteetti.



Kuva 2. MOVE-arkkitehtuuri keskittää verkkoon pääsyn politiikan. [23, sivu 7]

MOVE-arkkitehtuurissa verkossa yhdistetään kaikki verkon fyysiset osat toisiinsa siten, että erillisten sääntöjen ja hallinnointijärjestelmien sijasta on yksi järjestelmä, joka määrää pääsyn. Edelleen yritys voi valita, että esimerkiksi yrityksen omistamalla kannettavalla tietokoneella pääsyoikeudet vaikkapa tietylle palvelimelle ovat eri kuin työntekijän omalla älypuhelimella. Myös riippuvuus esimerkiksi käyttäjätunnuksesta tai kirjautumistavasta on valittavissa. Tästä on lisää luvussa 2.4.2. Ajatus on siinä, että keskitetty verkkoon pääsemisen hallinta on niin paljon yksinkertaisempi, että se parantaa ja selkiyttää yrityksen tietoturvaa sekä verkon hallintaa ja käytettävyyttä. Vikatilanteessa vian etsintä voidaan lähes poikkeuksetta aloittaa hallintajärjestelmästä tarkastamalla, minkälaiset oikeudet käyttäjä on kulloinkin saanut. Järjestelmän myös arvioidaan säästävän yritykseltä kustannuksia, kun kolmen-neljän lisenssin sijasta tarvitaan vain yksi. [23, sivut 7–9.]



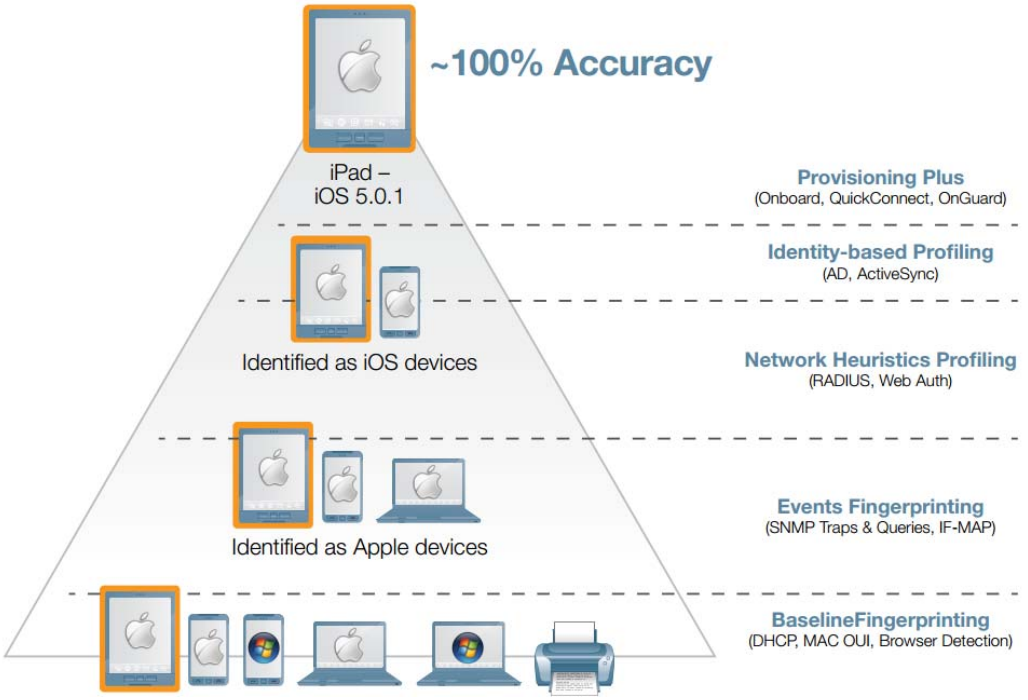
Kuva 3. MOVE-arkkitehtuuri ja siihen liittyvät komponentit. Kuvassa näkyvää Aruban langattoman verkon keskitettyä hallinta- ja valvontajärjestelmää AirWavea ei käsitellä tässä työssä. [23, sivu 8.]

2.4.2 ClearPass Policy Manager

ClearPass Policy Manager on alusta, joka ohjaa verkon tietoturvaa sääntöpohjaisesti. Sen kautta voidaan tehdä sääntöjä koko verkolle riippumatta siitä, onko kyseessä langallinen, langaton vai VPN-yhteys. Määriteltäviä sääntöjä eli politiikkoja voi olla käytössä useita samanaikaisesti. Verkkoon pääsyä voidaan tutkia ja rajata muun muassa käyttäjän roolin, laitteen tyypin ja terveyden, vuorokaudenajan tai verkkosijainnin pohjalta. ClearPass liitetään yrityksen muihin järjestelmiin yleisesti RADIUS-protokollalla. Se pitää sisällään paljon MDM:lle tyypillisiä ominaisuuksia, mutta ei toistaiseksi tue esimerkiksi laitteen etätyhjennystä tai sovellusten hallintaa. ClearPassin ensisijainen tarkoitus on korvata yrityksessä käytössä olevat vanhentuneet RADIUS-palvelimet ja yhtenäistää ne yhdeksi järjestelmäksi. ClearPassin yksi tärkeimmistä myyntivalteista on se, että se toimii kaikkien suurimpien valmistajien, kuten Ciscon, Juniperin, Enterasysin ja HP:n laitteista koostuvassa verkossa. Nojaamalla IEEE 802.1x -standardiin ja RADIUS-protokollaan ClearPass voidaan konfiguroida toimimaan myös monissa muissa monen valmistajan laitteista koostuvissa verkoissa. Mikäli verkossa on laitteita, jotka eivät tue 802.1x:ää, voidaan käyttää

esimerkiksi Captive Portal -tyyppistä, Internet-selaimessa tapahtuvaa kirjautumista ja autentikointia. [22.]

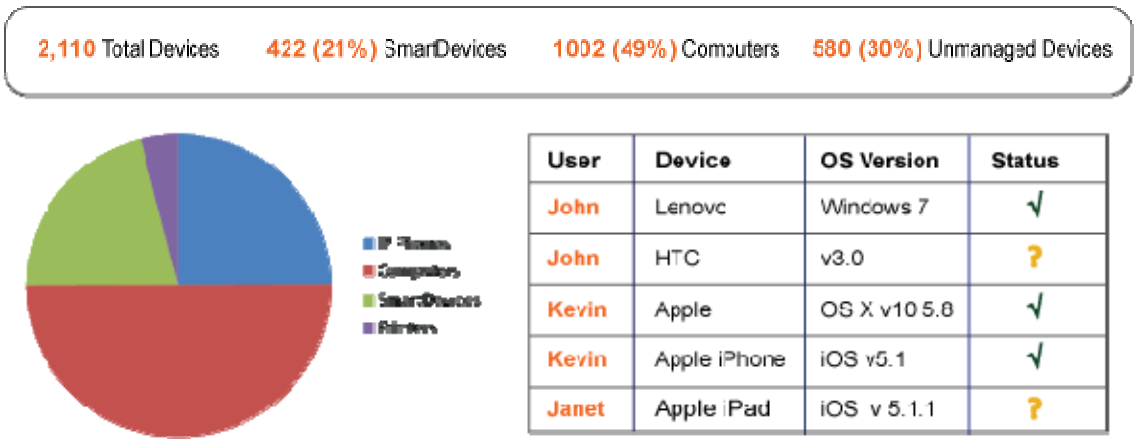
Policy Manager kerää käyttäjästä ja laitteesta tietoa 5-vaiheisen järjestelmän mukaan, jota kutsutaan profiloinniksi. Aivan aluksi verkkoon liitetty laite saa IP-osoitteen DHCP:ltä. Tällöin ClearPass tutkii DHCP:ltä saatuja tietoja ja katsoo MAC-osoitteen OUI:n. Käyttäjä ohjataan laitekohtaiseen Captive Portaliin tunnistautumaan. Selaimen tunnistuksella tarkkuutta saadaan parannettua. Tämän jälkeen SNMP:n avulla voidaan selvittää lisätietoja laitteesta, kuten esimerkiksi valmistajaan tai käyttöjärjestelmään liittyviä tietoja. Kolmannessa vaiheessa käyttäjä ohjataan OnBoardiin, jossa käyttäjä klikkaa laitteen selaimessa näkyvää rekisteröintipainiketta. Tällöin muilla kuin iOS-laitteilla käyttäjän tulee ladata QuickConnect-sovellus, joka tekee asetukset laitteeseen. Kun QuickConnect on asennettu, käyttäjä klikkaa selaimessa linkkiä, jolla saa ladattua varsinaisen verkkoprofiilin. ClearPass QuickConnect käynnistyy, jolloin käyttäjän tulee syöttää kirjautumistiedot. ClearPass tarkistaa esimerkiksi AD- tai LDAP-palvelimelta syötetyt kirjautumistiedot ja palauttaa WLAN-kontrollerille RADIUS acceptin tai rejectin riippuen kirjautumisen onnistumisesta. ClearPass voidaan myös konfiguroida käyttämään kaksivaiheista autentikointia, jolloin käyttäjältä vaaditaan vielä toissijainen kirjautuminen, esimerkiksi tekstiviestillä saatava kertakäyttösalasana. Kolmannen vaiheen aikana, joka on varsinainen AAA-prosessi, laitteesta ja käyttäjästä saadaan tietoja mm. RADIUS:n ja AD:n avulla. Normaalisti viimeisessä käyttäjän ja laitteen tunnistamisen vaiheessa, onboardingissa, laitteelle asennetaan QuickConnectin avulla tarvittavat sertifikaatit ja yhteysasetukset tarkastetaan sekä muutetaan mikäli tarpeen. IOS-laitteilla kirjautuminen onnistuu rajapinnan vuoksi OTA:na pelkän sertifikaatin lataamalla, mutta muille laitteille ClearPass QuickConnect täytyy asentaa. Tunnistusprosessin lopussa käyttäjän laite todennetaan IEEE 802.1x -standardilla verkkoon. Lähes sataprosenttiseen tunnistustarkkuuteen päästään, kun käyttäjä velvoitetaan asentamaan ja suorittamaan host checker -tyyppinen OnGuard-ohjelma, joka tarkistaa laitteen ja voi tutkia muun muassa virustorjuntaohjelmien ym. ajantasaisuuden. [24; 25, sivu 3; 26, sivut 21–26.]



Kuva 4. ClearPass profiloi käyttäjät ja laitteet viidessä vaiheessa, jonka aikana käyttäjä myös autentikoidaan verkkoon. Kuvan lähde: Aruba ClearPass Profile White Paper.

Kun tiedot käyttäjästä ja laitteesta on kerätty, Policy Manager sovittaa kerättyä tietoa sääntökokoelmaan palomuurin tavoin. Säännöt voivat olla tarpeesta riippuen yksinkertaisia tai hyvinkin monimutkaisia. Kun käyttäjälle laitteineen löytyy osuma säännöistä, Policy Manager antaa käyttäjälle roolin, jonka mukaan varsinainen verkkoon pääsy sallitaan. Rooleja on yleensä useita erilaisia, kuten esimerkiksi ylläpitäjät, talousosasto, kehitysosasto, vieras jne. Roolit on siis usein järkevä määrittää ryhmäjäsenyyden, kuten osaston perusteella.

Käyttäjälle annettu rooli sidotaan politiikkaan, joka määrää, minne kaikkialle käyttäjä pääsee yhdistämään. Englanniksi tätä kutsutaan Policy Enforcementiksi. Mikäli yrityksellä on kokonaan Aruban laitteista koostuva ympäristö, ClearPass voi tehdä palomuurisääntöjä suoraan Aruban WLAN-kontrollerin Policy Enforcement Firewalliin. Useimmiten yrityksillä on monen valmistajan laitteista koostuva verkko, jolloin rajaukset tehdään useimmiten VLANeja määrittämällä tai lähettämällä verkkolaitteille Access list-päivityksiä. VLANeissa pääsyä voidaan rajata verkosta erikseen löytyvällä palomuurilla, mutta kuten on jo aiemmin mainittu, VLANit eivät kunnolla skaalaudu mobiiliin ympäristöön, jonka vuoksi niiden kautta sulavaa BYOD-ympäristöä on vaikea ylläpitää. [22; 24.]



Kuva 5. ClearPass Policy Manager tunnistaa käyttäjän, laitteen ja muita oleellisia tietoja sekä sallii tai estää pääsyn verkkoon. Kuvan lähde Aruba Networks.

ClearPass Policy Manager tukee seuraavia autentikointitapoja: Active Directory, Kerberos, RADIUS, MS-CHAP, MS-CHAP (v2), EAP, PAP, LDAP, TACACS+, CHAP ja EAP-FAST. Policy Manageria voidaan hallita SNMP:llä, ja se tukee IEEE 802.1x -todennusta. [20; 24.]

Policy Managerin tärkeimpiä ominaisuuksia ovat sisäänrakennettu vierailijajärjestelmä (Guest), profilointi (Profile ja OnGuard), tunnetuimpien käyttöjärjestelmien (Windows, Android, iOS, OS X, Linux) automaattinen asetusten tekeminen (OnBoard), helppo sääntöjen luominen ja valvonta, helppokäyttöinen vianetsintäliittymä, sääntöjen simulointi ja testaus, reaaliaikainen käyttäjien ja laitteiden seuranta, raportit ja analyysit, hälytykset sekä mahdollisuus täyteen klusterointiin vikasietoisuutta varten. PolicyManagerin voi asentaa suoraan virtualisoidulle alustalle, kuten esimerkiksi Hyper-V:n tai VMWarelle, mutta siitä on suoraan myynnissä kolme vaihtoehtoa, joiden ominaisuudet on esitelty seuraavalla sivulla olevassa taulukossa. [20; 22.]

Taulukko 1. ClearPass Policy Managerin tekniset tiedot. Aruba Networks. Hinnat on etsitty verkosta ja arvioitu keskimääräinen hinta.

	ClearPass Policy Manager-500	**ClearPass Policy Manager-5000**	**ClearPass Policy Manager-25000**
CPU	(1) Dual Core Pentium 2.9-GHz G850	(1) Quad Core Xeon 2.66-GHz X3450	(2) Quad Core Xeon 2.66-GHz X5650
Memory	4 GB	8 GB	48 GB
Hard drive storage	(1) 3.5" SATA (7K RPM) 500-GB hard drive	(2) 3.5" SATA (7.2K RPM) 500-GB hard drive PERC H200 RAID-1 controller	(4) 2.5" SAS (10K RPM) 300-GB HotPlug hard drives PERC 6/I SAS RAID controller
Network ports	(2) Gigabit Ethernet	(2) Gigabit Ethernet	(2) Gigabit Ethernet
Maximum devices	500	5,000	25,000
Power consumption (maximum)	260 watts max	250 watts max	717 watts max
Power supply	Single	Single	Dual hot-swappable (optional)
Operating temperature	10º C to 35º C (50º F to 95º F)	10º C to 35º C (50º F to 95º F)	10º C to 35º C (50º F to 95º F)
Part number	CP-HW-500 or CP-VA-500 (virtual)	CP-HW-5K or CP-VA-5K (virtual)	CP-HW-25K or CP-VA-25K(virtual)
Approximate price (HW version)	6,000 USD	16,000 USD	60,000 USD

ClearPass Policy Managerin apuohjelmat (OnGuard, Onboard ja Guest) hankitaan erikseen yrityksen tarpeiden mukaan. Lisenssien koot riippuvat autentikoitavien laitteiden määrästä. ClearPassin hankintaa miettiessä onkin tärkeää aloittaa siitä, kuinka monta laitetta verkkoon liitetään.

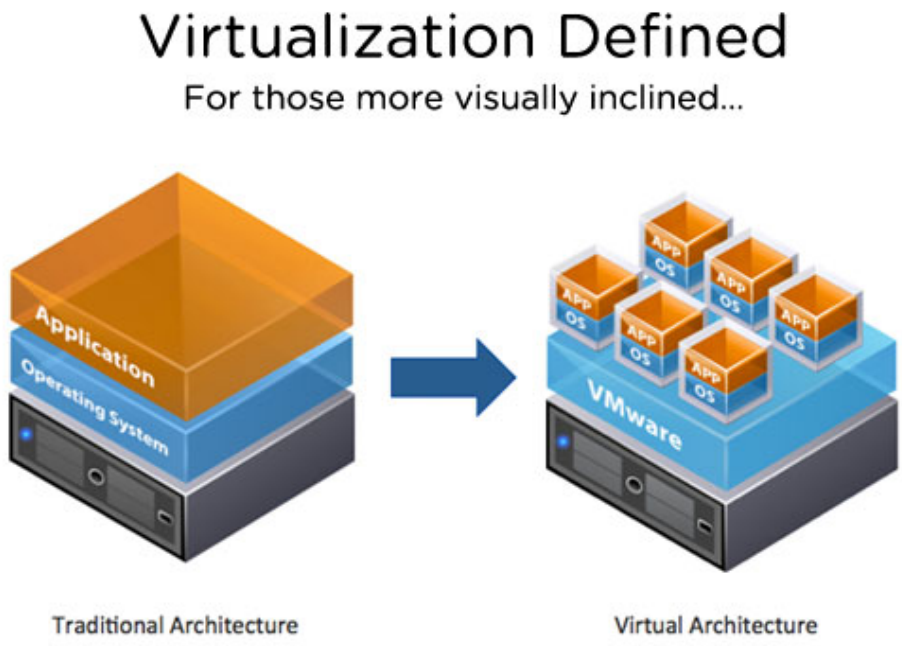
3 Virtual Desktop Infrastructure

3.1 Virtualisoinnin taustaa

Virtualisoinnilla tarkoitetaan usean virtuaalisen tietokoneen ajamista yhdellä tai useammalla fyysisellä tietokoneella. Kiinnostus virtualisointia kohtaan on kasvanut yrityksissä vuosi vuodelta. Perinteiset ongelmat, kuten hajautunut järjestelmä ja sitä kautta tulevat haasteet hallinnassa helpottuvat, kun palvelimia virtualisoidaan keskitettyyn järjestelmään. Kun perinteisiltä suoritinvalmistajilta, kuten Inteliltä ja AMD:ltä saapui markkinoille suorittimia, jotka tukevat virtualisointia, on virtualisoinnista tullut melko helposti toteutettava. Nykyään palvelimien laskentateho ja muu suorituskyky alkavat olla huomattavasti suurempaa luokkaa varsinaiseen tarpeeseen nähden. Raudan eli fyysisen laitteiston suorituskyky tarpeeseen nähden on siis kasvanut huimasti. Muun muassa laskentatehon kasvu on noudatellut Mooren lakia melko hyvin jo vuodesta 1975 alkaen. Mooren lain mukaan suorittimissa laskentaan käytettävien transistorien määrä kaksinkertaistuu noin kahden vuoden välein. Laskentatehon kasvu ei ole suoraan verrannollinen transistorien määrään, mutta tekniikan kehittyessä Mooren laki on pätenyt melko hyvin myös laskentatehon osalta. Raudan kapasiteetin ja tehon kasvu on saanut yritykset miettimään vaihtoehtoisia ratkaisuja. Virtualisoinnin tarpeet ovat yrityksen näkökulmasta ympäristöjen yksinkertaistamisessa ja taloudellisissa säästöissä. Yksi palvelin kuluttaa keskimäärin 300-500 W:n teholla sähköä. Lisää kuluja muodostuu laitteen hankinnasta, korjaamisesta, huolloista ja jäähdytyksestä. [27; 28.]

Otetaan esimerkki ja oletetaan, että yrityksellä on 50 erillistä palvelinta: Jokaisella palvelimella on omat edellä mainitut kulunsa, mutta palvelimien käyttöaste on tässä esimerkissä keskimäärin vain 10 %. Loput 90 % laskentatehosta, tallennuskapasiteetista, LAN-linkistä ym. resursseista laitteella on täysin käyttämättömänä. Lisäksi 50 fyysistä laitetta vaativat oman tilansa palvelinkeskuksesta. Olemassa on ratkaisu, virtualisointi, jolla mainitut 50 palvelinta voidaan pitää omina loogisina järjestelminään, mutta käyttää olemassa olevan raudan kapasiteetti tehokkaasti: hankitaan 5 fyysistä palvelinta, joihin virtualisoidaan kuhunkin 10 palvelinta. Lopputuloksena yrityksellä on 50 virtuaalipalvelinta, mutta vain kymmenesosa alkuperäisestä viidestäkymmenestä fyysisestä palvelimesta. Jokainen fyysinen palvelin käyttää keskimäärin 90–100 % resursseistaan. Virtuaalipalvelimia on myös helppo kloonata keskenään ja tarpeen tullen esimerkiksi siirtää. Fyysisiä laitteita

ei välttämättä tarvitse siirtää ollenkaan, vaan riittää että samanlainen virtualisointialusta on olemassa sekä vanhassa että uudessa sijainnissa. Tässä kohtaa tulee huomata, että todellisuudessa palvelimien käyttöasteet vaihtelevat käyttötarkoituksesta riippuen ja esimerkiksi tietokantapalvelin saattaa olla korkeallakin kuormalla jatkuvasti. [28.]



Kuva 6. Virtualisoinnissa perinteinen yksi tietokone – yksi järjestelmä -konsepti muutetaan pitämään sisällään monta täysin yksilöllistä järjestelmää. [28]

Virtualisointia voi toteuttaa usean eri valmistajan alustoilla, joista tässä työssä perehdytään hieman Vmwaren vSphereen. Muita markkinoilla olevia tarjoajia on muun muassa Microsoftin HyperV ja Citrixin XenServer. Virtualisointia voidaan myös tehdä yllä mainitun rautavirtualisoinnin lisäksi myös ohjelmistoille, muistille, levyjärjestelmille ja verkkoyhteyksille. Tehokkaasti virtualisoidussa ympäristössä käytetäänkin useampaa virtualisointitapaa samanaikaisesti, jolloin fyysisen laitteiston yksittäinen rikkoutuminen ei välttämättä vaikuta varsinaisen palvelun toimivuuteen mitenkään. Virtualisoitu alusta on myös helpompi varmuuskopioida talteen sellaisenaan ja nopea palauttaa uuteen virtuaalikoneeseen vikatilanteessa. Virtualisointi siis lisää vikasietoisuutta. [29.]

3.2 Työpöytävirtualisointi

Työpöytävirtualisoinnilla tarkoitetaan nimensä mukaisesti työntekijän työpöydän virtualisoimista. Tähän on monia syitä, kuten

- säästöt
- yhtenäistäminen
- tietoturva
- BYOD
- hallinta.

Työpöydän virtualisoinnilla yritykset pystyvät helposti ja keskitetysti hallinnoimaan työntekijöiden työympäristöä. Järjestelmien uudelleenasennus on vaivatonta ja varmuuskopiointi helppoa. VDI-ratkaisussa kaikki tieto on tallennettuna konesaliin, jolloin arkaluontoisen datan katoaminen ei ole mahdollista esimerkiksi työntekijän kannettavan tietokoneen kadotessa. Työntekijän näkökulmasta käytännöllisin asia on se, että omaan työpöytään pääsee yrityksen tietoturvapolitiikasta riippuen mistä tahansa käsiksi ja periaatteessa millä tahansa laitteella.

Tässä työssä perehdymme Virtual Desktop Infrastructureen eli VDI:hin. Se on yksi monista tavoista virtualisoida työpöytä. Seuraavaksi tutustutaan tarkemmin Citrixin myymiin vaihtoehtoihin virtualisoida työpöytä.

3.2.1 Hosted shared/pooled desktops

Jaettu yhteinen virtuaalityöasema on yksinkertaisin ja halvin tapa toteuttaa virtualisoitu työpöytä. Siinä kukin työntekijä saa jaetulta palvelimelta oman, samasta levykuvasta tehdyn työpöydän. Yksi palvelin pystyy käsittelemään maksimissaan noin 500 käyttäjää. Etuina ovat hallittavuus, keskitetyt toiminnot ja hinta, erityisesti alhainen TCO. Heikkoutena on muokattavuus käyttäjän mieltymysten mukaan. Tällainen ratkaisu soveltuu parhaiten yrityksen niille työntekijöille, jotka tekevät paljon staattista ja samankaltaista työtä. [30, sivu 3; 31, sivu 1.]

3.2.2 Hosted VDI desktops

VDI-työpöytä on tällä hetkellä yksi kiinnostavimmista työpöydän virtualisointitavoista. VDI-työpöytä on jokaiselle käyttäjälle omanlaisensa ja voi olla jopa kokonaan toinen käyttöjärjestelmä. Siihen pääsee tietoturvapolitiikasta riippuen yhdistämään mistä vain ja lähes millä laitteella tahansa. Ohjelmat ja varsinainen tallennettu data eivät koskaan poistu konesalista, jolloin tietoturva paranee. Lisäksi jokaisella käyttäjällä on mahdollisuus muokata työpöydästä omansa näköinen, jolloin käyttäjäkokemus vastaa paremmin omaa fyysistä työasemaa. IT:n näkökulmasta VDI on jaettu työpöytä -ratkaisun tavoin helposti hallinnoitava keskitetyn arkkitehtuurin vuoksi. Yhdelle palvelimelle voidaan viedä maksimissaan noin 150 VDI-työpöytää. VDI-työpöytä soveltuu hyvin koko yrityksen käyttöön, mutta muokattavuutensa vuoksi on tehokas ratkaisu erityisesti niille jotka tarvitsevat käyttöönsä erityisiä sovelluksia tai työkaluja. [30, sivu 4.]

3.2.3 Streamed VHD desktops

Puskuroitu VHD-työpöytä vastaa toiminnallisuudeltaan jaettua yhteistä virtuaalityöasemaa. Se on samanlainen kaikille käyttäjille ja toimii keskitetysti konesalista. Erona on kuitenkin se, että työasema puskuroidaan työntekijän omalle tietokoneelle paikallista suorittamista varten. Jaetun yhteisen virtuaalityöaseman resurssit tulevat konesalissa olevalta palvelimelta. Käyttäjämäärän kasvaessa palvelin kuormittuu jatkuvasti enemmän ja enemmän. Puskuroitu VHD-työasema antaa mahdollisuuden keskittää työpöydän, ohjelmistojen ja datan hallinnan konesaliin jättäen silti konesalissa olevan palvelimen pienemmälle kuormitukselle. Ohjelmien vaatima laskenta tehdään paikallisella työasemalla. Jokaisella käynnistyskerralla käyttäjällä on edessään puhdas työpöytä, jolla voi tehokkaasti suorittaa päivittäisiä työrutiineja. Puskuroitua VHD-työpöytää käyttäen konesalissa olevalle palvelimelle voidaan tallettaa jopa tuhansia työpöytiä. Malli soveltuu parhaiten usein muuttuvaan, mutta yhteisesti melko staattiseen ympäristöön, esimerkiksi opetuslaboratorioihin tai paikkoihin, joissa käyttäjiä on paljon ja ne vaihtuvat useasti. [30, sivu 5.]

3.2.4 Physical Desktops

Fyysiset työasemat ovat yritysmaailmassa ylivoimaisesti eniten käytössä oleva ratkaisu. Käytännössä tämä tarkoittaa, että jokaisella työntekijällä on oma, henkilökohtainen työnantajan hankkima tietokone. Yritykset eivät kuitenkaan usein salli

oman työaseman etäkäyttöä vaan työntekijät, joilla ei ole kannettavaa tietokonetta eivät käytännössä pääse siihen käsiksi kuin työpaikallaan. Etätyötä helpottamaan Citrixin fyysisen työpöydän ratkaisu avaa työntekijälle mahdollisuuden käyttää töissä olevaa tietokonetta etänä, kuten istuisi paikan päällä henkilökohtaisesti. Tietoturvan parantamiseksi ratkaisussa on mahdollisuus Windowsin etätyöpöydän tavoin rajoittaa kenellä käyttäjällä on pääsy laitteeseen. Erityisen lisäarvon tuo mahdollisuus 3D Workloads -optio, jolla 3D-grafiikkaa, raskasta videota tai muuta graafista suunnittelua voidaan tehdä helposti etätyönä. Citrixin ratkaisussa graafinen laskenta tehdään suorituspäässä ja vasta sen jälkeen siirretään etäyhteyden yli käyttäjälle. [30, sivu 6.]

3.2.5 Local virtual machine desktops

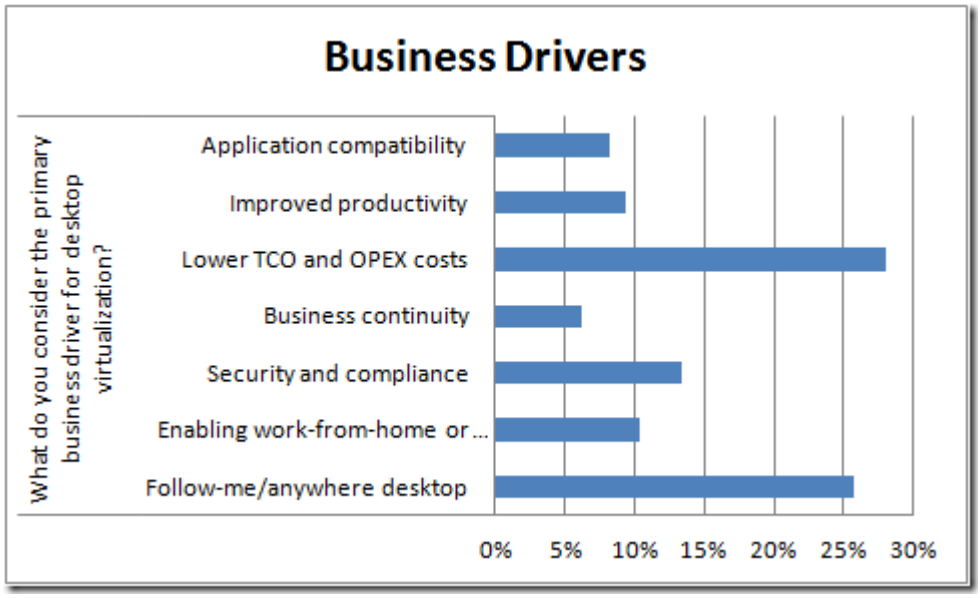
Paikallinen virtuaalikone on tehokas ratkaisu käyttäjille, jotka eivät ole jatkuvasti Internet-yhteyden ulottuvilla. Muiden työpöydän virtualisointimallien vaatiessa jatkuvan yhteyden yrityksen konesaliin soveltuu malli hyvin sellaisille työntekijöille, jotka ovat aika-ajoin verkon ulottumattomissa tai liian hitaan yhteyden takana. Paikallinen virtuaalikone sijaitsee käyttäjän omalla tietokoneella. Se ladataan ja asennetaan konesalissa sijaitsevalta palvelimelta työntekijän henkilökohtaiselle tietokoneelle, jonka jälkeen sitä voidaan käyttää tietokoneella, kuten mitä tahansa muuta paikallista käyttöjärjestelmää Internet-yhteydestä riippumatta. Kun yhteys konesaliin on saatavilla, virtuaalikone synkronoi tietonsa ja mahdolliset päivitykset konesalin kanssa automaattisesti. Tietokoneella voi olla myös erikseen työntekijän oma, henkilökohtainen käyttöjärjestelmä ja yrityksen toimittama virtuaalikone, jotka ovat täysin irrallisia toisistaan. Tällöin tietoturva ei vaarannu, vaikka työntekijä antaisi esimerkiksi lastensa käyttää tietokonetta. Työpöytämalli soveltuu parhaiten liikkuville työntekijöille tai niille, jotka tarvitsevat useamman käyttöjärjestelmän samalle tietokoneelle. Yrityksen IT:n näkökulmasta hallinta ja varmuuskopiot ovat edelleen keskitetyt ja tietokone päivittyy aina sen ollessa yhteydessä konesaliin. [30, sivut 6–7.]

3.3 Virtualisoinnin hyödyt ja haitat

Taulukko 2. Virtualisoinnin hyödyt ja haitat

Hyödyt	**Haitat**
Pitkällä aikavälillä operatiivisista kustannuksista saadaan säästöjä	Suuret alkuinvestoinnit
Helpottaa järjestelmien hallinnointia	Asettaa vaatimuksia tietoverkolle
Nopea ja helppokäyttöinen käyttäjälle	Ei toimi hyvin hitaiden tai laaduttomien yhteyksien yli
Tukee useita laitteita	Vaatii erillisen vastaanotin-ohjelman
Varmuuskopiointi ja palautus on helppoa	Keskitetty järjestelmä on riski, jos sitä vastaan hyökätään
Tavoitettavuus on korkea	Jos ympäristö menee kaatuu tai verkkoyhteydet katkeavat, kaikki toiminta lakkaa
Työasemien asennus on nopeaa	Palvelimien resurssit rajoittavat
Yksinkertaistettu järjestelmä helpottaa vianetsintää	Asiakas-palvelin –ajattelu ei ole kestävää kehitystä. Ihmiset haluavat omat laitteet ja sovellukset.
Työpöytävirtualisoinnissa työpöytä on samanlainen riippumatta käyttäjän laitteesta	Ei pysty korvaamaan tuotantojärjestelmiä, kuten automaatioverkkoja.

Virtualisointi tuo mukanaan lukuisia merkittäviä hyötyjä. Ensiksi pitää kuitenkin erottaa palvelin- ja työpöytävirtualisoinnit toisistaan. Ensisijaisesti yritykset siirtyvät virtualisoituun työpöytään kahdesta syystä: sillä tavoitellaan taloudellisia säästöjä ja saavutettavuuden kasvattamista. Taloudellisia säästöjä saadaan lukuisista eri kohteista, joita ovat muun muassa työasemahankintakulujen väheneminen, keskitetyn hallinnan mukanaan tuomat hallinnolliset säästöt, energian kulutukseen liittyvät säästöt sekä säästöt IT:n työajassa. Palvelinpuolella taloudellisia säästöjä syntyy esimerkiksi fyysisten palvelimien määrän pienenemisestä. Fyysisten palvelimien vähentyessä vähentyvät kulut niin energian, hallinnon, hankintojen kuin huoltojenkin osalta. Hallinnon osalta asiassa on myös kääntöpuoli: Virtuaalipalvelin katsotaan yleensä hyvin kriittiseksi järjestelmäksi, jolloin huoltosopimuksen täytyy olla parhaalla mahdollisella tasolla. Yksittäisten, ei-virtualisoitujen palvelimien osalta voidaan määritellä, kuinka kriittinen kukin palvelin on ja ostaa niihin tarpeen mukaiset huoltosopimukset. Tästä huolimatta pelkästään palvelinkeskuksissa virtualisointi luo merkittäviä säästöjä jo pelkän sähkö- ja jäähdytysenergian osalta. [28; 31.]



Kuvio 1. Työpöytävirtualisoinnin tavoitteet. [32]

Gartnerin loppuvuodesta 2012 julkaistussa kyselyssä (Desktop Virtualization Trends at Gartner Data Center, C. Wolf) kysyttiin työpöytävirtualisoinnin tavoitteita bisneksen kannalta. Oleellisimpana nähtiin alhaisempi TCO eli omistuskulut ja OPEX eli käyttökulut, toiseksi tärkeimpänä mistä tahansa tavoitettavissa oleva työpöytä. Kolmantena ovat turvallisuuteen liittyvät asiat. [32.]

Työpöytien virtualisointi ja niiden keskittäminen tuovat muitakin merkittäviä etuja säästöjen lisäksi. IT-yksikön hallinnointi helpottuu huomattavasti, erityisesti jos sovelletaan esimerkiksi Citrixin jaetun virtuaalityöaseman mallia. Mallissa on vain yksi Windows-kuva, jossa ovat samat ohjelmistot ja samat asetukset käyttäjästä riippumatta. Yhden käyttöjärjestelmäkuvan käyttö johtaa siihen, että ohjelmistojen ja käyttöjärjestelmän hallinta on vaivattomampaa ja päivitysten testaamiseen menee murto-osa ajasta verrattuna tilanteeseen, jossa käyttäjillä saattaa olla eri versioita ohjelmistoista ja käyttöjärjestelmistä. Lukuisten variaatioiden testaamisen sijasta IT:n tarvitsee testata vain yksi kokoonpano ennen julkaisua. Myös varmuuskopioiden ja palautusten tekeminen on helppoa, koska käyttäjän työpöytä ja tiedostot voidaan kopioida sellaisenaan ja tarvittaessa palauttaa vaikka kokonaan toiselle fyysiselle isäntälaitteelle eli palvelimelle. Jos varmuuskopiot tehdään riittävän usein, ei palautustilanteessa käyttäjän näkökulmasta muutu välttämättä mikään. Kun tätä vertaa esimerkiksi tilanteeseen, jossa IT käy tyhjentämässä käyttäjän tietokoneen ja asentaa sinne kaiken uudestaan, on käyttäjältä todennäköisesti hävinnyt sekä päivä työaikaa että tärkeitä tiedostoja. [31, sivut 5–6.]

Työpöytävirtualisoinnin yksi kiinnostavimmista hyödyistä on kuitenkin tuki erilaisille alustoille. Samassa aihepiirissä voidaan puhua kahdesta asiasta: virtualisointialustan mahdollisuuksista toisin sanoen, mitä käyttöjärjestelmiä voidaan virtualisoida ja työpöytävirtualisoinnin tapauksessa, millä laitteilla virtuaaliseen työpöytään voidaan yhdistää. Pääsääntöisesti virtuaalialustoille voidaan asentaa lähes mitä käyttöjärjestelmiä tahansa, joten tässä työssä sivuutetaan aiheen syvempi tarkastelu. Sen sijaan VDI:n tutkimisen kannalta on oleellista tutkia ohjelmia, joilla virtuaaliseen työpöytään voidaan yhdistää. Etuna on, että nykyään lähes millä tahansa laitteella voi käyttää virtuaalityöpöytää. Laite voi olla esimerkiksi Windows, Linux, Mac, Android-tabletti tai iPhone. Tämä tekee erityisesti saavutettavuuden erityisen helpoksi ja samalla tärkeäksi hyödyksi virtuaalityöpöytien kanssa. Vastaanottimista tarkastelen Citrix Receiver -ohjelmistoa myöhemmin työssä. [31, sivu 2.]

Virtualisoinnilla on myös haasteensa BYOD:n tavoin. Haasteita tulee vastaan jo vanhojen järjestelmien siirrossa virtualisoituun ympäristöön, jossa monimutkaiset lisensointikuviot ja yhteensopivuusongelmat saattavat tehdä virtualisointiprojektista pitkän. Alkuinvestoinnit ovat yleensä korkeat, koska useimmiten palvelinkeskus uusitaan täysin vastaamaan virtualisoinnin tarvetta. Vaikka palvelimet nykyään virtualisoidaan lähes aina, on varmuuskopioinnissa omat haasteensa. Varmuuskopiot pitää ottaa nimenomaisesti virtuaaliympäristöstä, eikä perinteiseen tapaan palvelimelta. Palvelimelta ajettavat varmuuskopiot eivät ota huomioon sitä, että järjestelmä on täysin looginen. Lopputuloksena varmuuskopioista puuttuu virtuaalijärjestelmän varmuuskopio, jolloin palautustilanteessa se pitää rakentaa alusta. [33, kohta 4.]

Verkkoyhteydet ovat virtualisoinnin ja erityisesti työpöytä- ja sovellusvirtualisoinnin suurimpia riskejä. Jos verkkoyhteydet eivät toimi, käyttäjien virtuaaliset työpöydät eivät toimi eikä virtualisoituihin palvelimiinkaan saa yhteyttä. Virtualisoidut työpöydät johtavat lähes poikkeuksetta siihen, ettei offline-työskentely ole mahdollista. Verkkoyhteyksien ei tarvitse olla välttämättä edes täysin poikki vaan riittää, kun suunnitteluvaiheessa ei ole otettu huomioon verkolle asetettavia vaatimuksia ja pääsee syntymään pullonkauloja. Esimerkiksi virtuaalipalvelimet, jotka käyttävät verkkolevyjärjestelmää, SAN:ia, kärsivät merkittävästi yhteysvioista. Kansainvälisesti toimivilla yrityksillä on ollut haasteena WAN-yhteyksien hitaus ja laaduttomuus. Koska virtuaalinen työpöytä on reaaliajassa toimiva palvelu, se on erittäin altis verkon ongelmille. [33, kohdat 1 ja 2; 8.]

Virtuaalityöpöytien kohdalla valmistajat usein hehkuttavat käytettävyyttä laitteella kuin laitteella. Herää kuitenkin kysymys, missä vaiheessa työpöytä ei ole enää käytettävissä laitteen asettamien rajoitusten vuoksi. Windows-työpöydän käyttö on mahdollista esimerkiksi Citrixin järjestelmässä Receiver-ohjelmiston kautta, mutta mikäli käyttävänä laitteena on iPhone, voidaan jo ruudun kokoa pitää täysin rajoittavana tekijänä. Samantyyppinen rajoittavuus pätee myös tabletteihin ja muihin laitteisiin, joista ei esimerkiksi näppäimistöä löydy. Työpöytävirtualisoinnilla on siis täsmälleen sama haaste kuin BYOD:lla. Mikäli käytettävää sovellusta tai työpöytää ei ole suunniteltu käytettäväksi esimerkiksi kosketusnäytöllä, ei se realistisesti myöskään käytettävä ole. Windows 8 helpottanee hieman tilannetta käyttöjärjestelmätasolla, mutta sovellusten osalta ongelma ei katoa vielä minnekään vaan sovelluksissa joudutaan silti turvautumaan SaaS-ratkaisuihin. Virtualisointiratkaisua miettiessä yrityksen tuleekin harkita, minkälaisilla laitteilla ympäristöjä voidaan aidosti käyttää. Mikäli tavallinen käyttäjä saa yhdistää vain virtuaaliseen Windows-työpöytäänsä, kannattaa suunnitteluvaiheessa harkita, salliiko pääsyä esimerkiksi älypuhelimilla lainkaan.

3.4 Citrix XenDesktop

3.4.1 XenDesktopin ominaisuudet

Citrixin XenDesktop on Citrixin vastaus BYOD hypeen. XenDesktop valittiin työhön, koska se on markkinajohtaja sektorillaan. Se vastaa samalla myös hallintaongelmiin kirjavan laite- ja ohjelmistokannan sekä työpöytien osalta. XenDesktopin voi tällä hetkellä asentaa usealle eri alustalle, kuten Citrixin omalle XenServerille tai Vmwaren vSpheren päälle. Tässä työssä tutkitaan XenDesktopin käyttöönottoa Vmware-ympäristössä Vmwaren markkina-aseman vuoksi. [34.]

XenDesktop pitää sisällään jo kohdassa 3.2 esitellyt virtualisointivaihtoehdot. Virtuaaliseen työpöytään voidaan yhdistää yrityksen sisäverkossa tai etänä esimerkiksi Citrix Remote Access Gatewayn kautta. Jotta työasemaan voidaan yhdistää, täytyy käyttäjän laitteella olla asennettuna Citrixin Receiver-ohjelmisto. Lisäksi on olemassa mahdollisuus korvata yrityksen tietokoneet kevyillä päätteillä (thin client tai zero client), jotka yhdistävät suoraan XenDesktop-järjestelmään ja niitä voidaan käyttää vain VDI-työpöytään yhdistämiseen. Kevyiden päätteiden käyttöönotto virtualisoidussa ympäristössä on suositeltavaa, koska ne ovat nopeita ja halpoja verrattuna täysiin tietokoneisiin. XenDesktop tukee myös 3D-grafiikoita, USB-laitteiden käyttöä,

roamingia, nopeampaa Windowsin käyttäjäprofiilien lataamista ja multimediatoimintoja kuten videota ja ääntä. Tavoitteena onkin, että käyttäjälle käyttökokemus olisi samanlainen kuin vanhalla täystyöasemalla istuessa, mutta erona nopeus. [30; 31, sivut 2–3.]

Verkkopuolella XenDesktopin ominaisuuksia ovat liikenteen salaus, kaksivaiheinen autentikointi, verkon käytön optimointi ja sisäänrakennettu SSLVPN-ominaisuus etäyhteyksiä varten. Erityisesti IT-yksikön kannalta tärkeitä ominaisuuksia on keskitetty salasanojen, datan ja käyttäjien hallinta, automaattinen virtuaalityöpöytien asennus käyttäjille, sisäänrakennettu helpdesk-ominaisuus sekä valvonta ja lokitusominaisuudet. [31, sivut 4–5.]

XenDesktopin saa hankittua kolmena eri versiona, jotka ovat VDI-, Enterprise- ja Platinum-versiot. Jokaisessa versiossa on hieman eroja toisiinsa, mutta oleellisimmat erot ovat, että VDI-versio on pelkästään VDI eikä pidä sisällään muita virtualisointivaihtoehtoja, kuten jaettua yhteistä työpöytää tai paikalliselle tietokoneelle tuotuja virtuaalikoneita. VDI-versiosta puuttuu myös pelkkien ohjelmien (ei koko käyttöjärjestelmän) virtualisointi. Tässä työssä ei perehdytä ohjelmien virtualisointiin tarkemmin. Enterprise- ja Platinum-versioiden tärkein eroavaisuus lienee sisäänrakennettu Citrix Access Gateway SSLVPN, joka löytyy ainoastaan Platinum-versiosta. Sama pätee myös muutamaan muuhun tietoturvaominaisuuteen, jotka on keskitetty salasanojen hallinta, ohjelmien valvonta ja politiikkapohjainen pääsynhallinta. [35; 36.]

3.4.2 XenDesktopin vaatimukset

XenDesktop vaatii alustalta paljon resursseja. Koska kyseessä on yleensä täysin palvelinkeskuksessa olevilla palvelimilla ajettava ympäristö, ja siinä saattaa olla satoja, jollei tuhansia virtuaalityöpöytiä, on oleellista varmistaa, että riittävät resurssit on saatavilla. Mikäli Vmwaren käyttämät isäntäkoneet eli ESXi:t ylikuormittuvat, tulee ympäristöstä epävakaa, joka saattaa aiheuttaa suuria ongelmia kaikilla käyttäjillä kaikissa palveluissa, joita virtuaalialustalta ajetaan.

Taulukko 3. Citrixin suositukset Vmwarella ajettavalle XenDesktopille. [37]

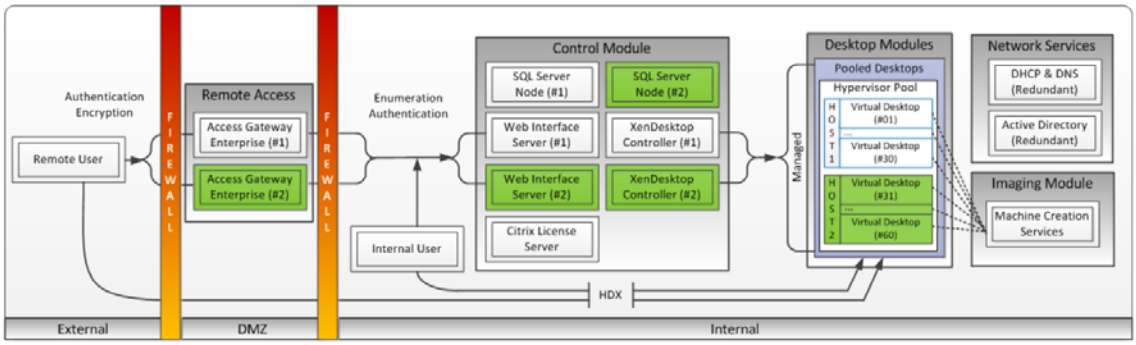
Tyyppi	**Määrä/Koko**
Klustereita	2-3 alkaen
ESXi-isäntäkoneita	8 per klusteri
Virtuaalisia työpöytiä per fyysinen suoritinydin	2-10 kappaletta riippuen käyttäjien aiheuttamasta kuormasta
Suoritin	Intel VT tai AMD-V (64-bit). Eri valmistajien suorittimia ei voi olla samassa klusterissa.
Muisti	Minimissään 2 Gt. Skaalataan virtuaalisten työpöytien vaatimusten mukaan.
Levytila	Minimissään 5,2 Gt, RAID ja thin-provisioning. Skaalataan muistin tavoin.
Verkkokortit	4 kpl

3.4.3 XenDesktopin asennus

XenDesktopin asennus alkaa lisensoinnin valinnalla. Kun varsinainen XenDesktop-versio on valittu, pitää yrityksen miettiä, millainen lisensointimalli otetaan käyttöön. Citrix tarjoaa XenDesktopin lisensointivaihtoehtoina per käyttäjä lisensointia, per laite lisensointia sekä per yhteys lisensointia. Käytännössä käyttäjäkohtainen lisensointi on paras valinta, kun jokainen tarvitsee oman VDI:n ja käyttää sitä usealla laitteella. Laitekohtainen lisensointi on paras valinta, kun useampi työntekijä käyttää samaa tai samoja laitteita VDI:hin yhdistämiseen. Yhteyspohjainen lisensointi on paras valinta, kun käyttö ja käyttäjät ovat satunnaisia ja vaihtuvuus on suuri. Kolmas vaihe ostoprosessissa on ohjelman valinta. Vaihtoehtoina on yksityisen sekä julkisen sektorin ohjelmat. Käytännössä suuryritys valitsee poikkeuksetta yksityisen sektorin ohjelman ja sen sisältä ELA:n (Enterprise Licence Agreement). Julkisen sektorin ohjelmasta löytyy kunnille, valtioille, oppilaitoksille ja voittoa tavoittelemattomille järjestöille räätälöidyin hinnoin varustettuja lisenssejä. Lisenssien hinnat vaihtelevat lisenssityypin ja tilattavan määrän mukaan eikä tarkkaa hinnastoa ole julkaistu. Aloituspaketiksi suunnattu EASY-lisenssi per käyttäjä tai laite maksaa Suomessa vuodessa VDI-versiona noin 75 euroa, Enterprise-versiona noin 180 euroa ja Platinum-versiona noin 280 euroa. [35; 38.]

Tässä tutkimuksessa seurataan Citrixin toimittamia ohjeita XenDesktopin täysversion eli Platinum-tason lisenssin asentamiseen Vmwaren virtualisointialustalle. Tämän jälkeen luvussa 5 arvioidaan käyttöönottoa asennuksen kannalta. XenDesktopin versio on 5.5, ja se asennetaan vSphere 5 -ympäristöön. Asennusdokumentissa oletetaan, että Vmware-ympäristö on asennettu ja siinä on riittävästi resursseja. Lisäksi oletetaan, että verkosta löytyy valmis ja toimiva AD-ympäristö ja että Microsoftin tuotteisiin vaadittavat lisenssit on hankittu.

XenDesktopin asennuksessa asennetaan useita Microsoft Windows 2008 -palvelimia sekä Citrixin toimittamia komponentteja. Jokainen komponentti asennetaan omana virtuaalikoneenaan. Lisäksi asennetaan Windows 7 -versio, josta tulee pohjakuva varsinaisille VDI-työpöydille. Asennustyö vaatii aikaa ja tietämystä Windows-palvelimista sekä Vmwaresta. Kokonaisuudessaan työssä asennetaan 6 uutta palvelinta jo olemassa olevan AD:n lisäksi sekä yksi Windows 7 -käyttöjärjestelmä.



Kuva 7. Asennettava XenDesktop-arkkitehtuuri. [39 sivu 5.]

Ensimmäisenä asennetaan Microsoft SQL 2008 R2 -palvelin. SQL toimii runkona koko VDI-järjestelmälle eikä ilman sitä VDI voi toimia. SQL-palvelin voi olla myös 2003 tai 2008 versiota, kunhan Service Pack 2 on asennettuna. SQL-palvelinta varten luodaan uusi virtuaalikone, jonne varsinainen SQL-palvelu asennetaan. SQL-palvelun asennus on melko suoraviivaista, mutta oleellista on huomata asentaa ominaisuus Database Engine Services. [39, sivut 8–14.]

SQL-palvelimen asentamisen jälkeen asennetaan Citrix Licensing Server, tässä tapauksessa versio 11.9. Licensing Server vastaa verkossa olevien Citrixin ja vSphere 5 -tuotteiden lisensoinnista. Tässä työssä lisensointipalvelin asennetaan samalle laitteelle SQL-palvelimen kanssa. Ensimmäisenä palvelimelle lisätään .NET 3.5.1 -ominaisuus, jonka mukana palvelimelle asentuu myös IIS-rooli. Tärkeää on varmistaa, että IIS-asennuksen yhteydessä .NET Extensibility & Request Filtering on valittuna. Kun asennukset ovat valmiita, asennetaan Licensing Server 11.9 Citrixin toimittamalta asennusmedialta. Asennuksessa asetetaan ylläpitäjän salasana, joka on syytä tallettaa myöhempää käyttöä varten. Asennuksen jälkeen tulee varmistaa, että mikäli käytetään tehdasasetettuja portteja, tulee Windowsin palomuurista avata portit 27000, 7279 ja 8082, jotta lisensointi on mahdollista. Kun asennustoimenpiteet on tehty, lisenssipalvelimelle viedään ostettu lisenssi License Administration Consolen kautta. [39, sivut 15–23.]

Desktop Controller huolehtii käyttäjien pääsystä, resurssien jakamisesta ja ohjaa käyttäjät oikeaan VDI-työpöytään sisäänkirjautumisessa. Samalle palvelimelle asennetaan myös Citrixin Desktop Director ja Desktop Studio -ohjelmistot. Palvelin on tässä työssä Windows Server 2008 R2. Desktop Director tarvitsee web palvelin -roolin (IIS), se asennetaan ensimmäiseksi server managerin kautta. IIS-roolin asentamisen jälkeen on suositeltavaa viedä SSL-sertifikaatti luotetuksi sertifikaatiksi tai allekirjoituttaa sertifikaatti kaupallisella myöntäjällä. Seuraavaksi palvelimelle asennetaan XenDesktopin ohjelmistot XenDesktop Controller, Desktop Studio ja Desktop Director Citrixin toimittamalta medialta. Palvelun toimivuuden varmistamiseksi allokoidaan toinen virtuaalinen Windows 2008 R2 -palvelin, jonne asennetaan toinen XenDesktop Controller samalta medialta kuin yllä. Asennettavat komponentit ovat XenDesktop Controller ja Desktop Studio. Koska toiselle palvelimelle ei asenneta IIS-roolia, palomuurista on syytä varmistaa avaus portille 80. [39, sivut 24–37.]

Asennusten valmistuttua luodaan XenDesktop site ensisijaisen Desktop Controllerin kautta. Desktop Studio -ohjelmistosta valitaan Desktop Deployment, jonka jälkeen tehdään asetukset, kuten nimeäminen, SQL-yhteys, lisenssien valinta sekä virtualisointialustan ja varsinaisten VDI-työpöytien perusasetukset Vmware-klusterissa. Tämän jälkeen toissijainen Desktop Controller liitetään äsken luotuun ympäristöön käyttämällä toissijaiselle Desktop Controllerille asennettua Desktop Studio -ohjelmistoa. [39, sivut 8–44.]

Jotta käyttäjät pääsisivät kirjautumaan VDI-työpöytäänsä käyttäen normaalia Internet-selainta, tarvitaan asennus Web Interfacelle. Web interface asennetaan tyypillisesti omalle palvelimelleen, tässä tapauksessa uudelle Windows Server 2008 R2 -palvelimelle. IIS-roolin asennuksen jälkeen palvelimelle asennetaan Microsoft Visual J# .NET 2.0 Citrixin asennusmedialta. Tämän jälkeen asennetaan varsinainen Citrix Web Interface, jonka kautta VDI-palveluihin voidaan yhdistää selaimella. Kun asennus on valmis, käytetään Web Interfacen Management-työkalua sivuston luomiseen. Sivuston luonnissa kysytään, missä autentikointi tehdään. Tyypillisesti se tapahtuu Web Interfacessa. Sivuston luomisen jälkeen sivusto linkitetään Desktop Controllereihin, tehdään autentikointiin liittyviä asetuksia ja valitaan sivuston ulkoasu. [39, sivut 45–57.]

Citrix Merchandising Server tarjoaa ylläpitäjille tavan toimittaa Citrix Receiver -ohjelmisto ja sen asetukset sekä päivitykset käyttäjille. Merchandising Server ladataan Citrixin lataussivulta Internetistä ja viedään Vmwareen OVF-kuvana. Tuomisen jälkeen varmistetaan, että Merchandising Serverillä on käytössään kaksi virtuaalista

prosessoria ja vähintään 4 gigatavua muistia. Tämän jälkeen palvelin käynnistetään ja siihen tehdään verkkoasetukset konsolin kautta. Kun verkkoasetukset on tehty, pääsee laitteeseen yhdistämään selaimella https-protokollalla ja kirjautumaan tehtaan root-tunnuksilla. Laitteelle tehdään AD-asetukset, jotta sinne voidaan kirjautua käyttäen AD-tunnuksia. Merchandising Serverille tehdään myös joukko muita asetuksia, joilla määritellään ladattavat ohjelmistot, säännöt siitä, kuka tai ketkä ohjelmiston voi ladata sekä jakelun asetukset. [39, sivut 58–74.]

Tässä vaiheessa asennusprosessia on asennettu suurin osa oleellisista XenDesktopin vaatimista komponenteista. VDI-ympäristöä ajatellen tärkein komponentti on kuitenkin asentamatta. Käyttäjien Windows 7 -käyttöjärjestelmä luodaan asennetun järjestelmän pohjalta. Tämä niin sanottu isäntäkuva (master image) toimii pohjana kaikille uusille VDI-työpöydille. Isäntäkuvan käyttöönottamiseksi luodaan uusi virtuaalikone, johon asennetaan tässä työssä Windows 7 64bit -järjestelmä. Oletusasetuksina suositellaan, että isäntäkuvalla olisi 2 virtuaalista suoritinta ja vähintään 2 gigatavua muistia. Kiintolevyn kooksi määritellään 24 gigatavua ja verkkoadapteriksi kannattaa valita VMXNET 3. Kun isäntäkuvan asentaminen on tehty järjestelmään, kirjaudutaan ja sinne asennetaan Citrixin toimittamalta medialta User Profile Manager. Ohjelma mahdollistaa ylläpitäjille helpon tavan hallita henkilökohtaisia asetuksia VDI:ssä. User Profile Manager vaatii myös AD:n päässä lukuisia asetuksia, joita ei käydä tässä yhteydessä tarkemmin läpi. [39, sivut 75–90.]

Active Directoryyn on suositeltavaa tehdä optimointeja koskien Windows 7 VDI-työasemia. Tehtävät Group Policyn määrittelemät asetukset lisäävät järjestelmän tehokkuutta ja poistavat päällekkäisyyksiä esimerkiksi varmuuskopioinnissa. Group Policystä on suositeltavaa määritellä pois päältä automaattiset päivitykset ja järjestelmän palautus. Lisäksi kannattaa tehdä yrityskohtaisia asetuksia esimerkiksi työpöydän lukitsemisen ja raportoinnin osalta. Citrix ohjeistaa myös tekemään lukuisia optimointeja Group Policyn rekisterieditorin kautta. Tällaisia asetuksia ovat esimerkiksi muistiin ja verkkoon liittyvät hienosäädöt. Ensisijaisesti yrityksen oma tietoturva- ja IT-politiikka määräävät, minkälaisia asetuksia AD:n kautta jaetaan. [39, sivut 91–101.]

Isäntäkuvalle tulee asentaa Vmware Tools -ohjelmisto. Ohjelmisto varmistaa muun muassa sen, että tietokoneen ajurit ovat oikeat. Windows 7 -isäntäkuvalle asennetaan myös Citrixin medialta Virtual Desktop Agent -sovellus. Ohjelmistoon määritellään Desktop Controllerit ja asennus tekee tarvittavat palomuurisäännöt automaattisesti. Tämän jälkeen isäntäkuvaa optimoidaan. Palveluiden hallinnasta sammutetaan

palveluita, jotka saattavat häiritä VDI-ympäristön toimintaa. Lisäksi tehdään lukuisia muita asetuksia, joista mainittakoon sivutiedoston koon määrittäminen vakioksi, joka on erittäin tärkeää. Koneelle myös asennetaan Service Pack 1- sekä VMXNET 3 -adapteriin liittyvä hotfix-päivitys. Kun optimointi on tehty, isäntäkuva liitetään domainiin. [39, sivut 102–118.]

Etätyöskentelyä varten XenDesktop-ympäristöön asennetaan Citrix Remote Access Gateway tuotenimeltään NetScaler VPX. Virtuaalinen versio ladataan Citrixin lataussivulta ja viedään Vmwareen OVF-tuomisen kautta. Tuonnin jälkeen virtuaalikone käynnistetään ja sinne määritetään verkkoasetukset konsolin kautta. Kun verkkoasetukset on tehty, laite uudelleenkäynnistyy ja siihen yhdistetään https-protokollalla selainta käyttäen. Laitteeseen tehdään useita asetuksia, kuten MIP/SNIP, lisensointi ja käynnistetään Access Gateway -ominaisuus. Access Gatewaylle luodaan sertifikaatti, joka allekirjoitetaan esimerkiksi AD-palvelimella. Sertifikaatin allekirjoituksen jälkeen luodaan uusi virtuaalinen palvelin, jolle määritetään oma IP, äskettäin allekirjoitettu sertifikaatti, tehdään LDAP-asetukset AD-yhteyttä varten ja määritellään Web Interface -palvelimelta sivu, joka esitetään etänä kirjautuvalle käyttäjälle. Asetusten tekemisen jälkeen kirjaudutaan Web Interface -palvelimelle ja luodaan uusi sivu, jossa autentikointi tapahtuu Access Gatewayllä. Access Gatewayn kirjautumissivu kerrotaan Web Interface -palvelimelle uuden sivun asetusten teon yhteydessä. Muuten uuden sivun luominen noudattelee jo aiemmin luotua sivua. [39, sivut 119–146.]

Seuraavaksi määritellään työpöytien varsinainen jakaminen käyttäjille. Työpöydät jaetaan Desktop Controllerin Desktop Studio -ohjelmistolla. Tässä esimerkkityössä yksinkertaistuksen vuoksi työpöytien tyyppi on pooled, jossa virtuaalityöpöydät jaetaan käyttäjille satunnaisesti eivätkä ne säilytä mitään järjestelmään tehtyjä muutoksia uloskirjautumisen jälkeen. Työpöydät voivat myös olla esiasetettuja tietyille käyttäjille tai ne voidaan määrittää asettumaan tietylle käyttäjälle ensimmäisen yhdistämisen yhteydessä. Näissä työpöytätyypeissä myös säilyy käyttäjän tekemät asetukset. [39, sivut 146–147.]

Desktop Studiossa valitaan aiemmin luotu Windows 7 -isäntäkone Vmware- klusterista. Seuraavassa ikkunassa määritellään luotavien virtuaalityöpöytien määrä ja näiden resurssiasetukset. Tätä tehtäessä on syytä varmistaa, että Vmware-klusterissa on riittävästi resursseja kaikkien työpöytien luomiseksi. Käyttäjät liitetään työpöytiin joko antamalla Desktop Studion luoda tiettyyn ryhmään kokonaan uudet käyttäjät tai

käyttämällä olemassa olevaa käyttäjäryhmää. Mikäli määritellään kokonaan uusia käyttäjätunnuksia, voi Desktop Studiossa määrittää tunnusten nimeämistavan, jolloin tunnuksia ei tarvitse luoda yksitellen. Luotaville virtuaalityöpöydille annetaan katologinimi, jonka perusteella ne voidaan tunnistaa ja erottaa mahdollisesti muista virtuaalityöpöydistä. Kun työpöydät on luotu, liitetään katalogin työpöydät käyttäjiin. Tämän jälkeen koko XenDesktopin asennusprosessi on kokonaisuudessaan valmis. [39, sivut 148–152.]

Ympäristön asentamisen jälkeen käyttäjät hakevat päätelaitteelleen Citrix Receiver -ohjelmiston Merchandising Serveriltä ja kirjautuvat siihen. Tämän jälkeen sisäinen pääsy tapahtuu suoraan Web Interface -palvelimen osoitetta käyttäen ja vastaavasti etäkäyttö Access Gatewayn osoitetta käyttäen. Kummassakin tapauksessa käyttäjä, jolle on määritetty VDI aiemmin, näkee kirjautumisen jälkeen työpöydän kuvakkeen, josta klikkaamalla Citrix Receiver käynnistyy ja avaa virtuaalityöpöydän. [39, sivut 152–156.]

Taulukko 4. Työssä asennetut XenDesktopin vaatimat virtuaalikoneet.

Nimi	**Tyyppi**	**Kuvaus**	**Määrä**
SQL-palvelin	Windows Server 2008 R2	Tietokantapalvelin XenDesktopia varten.	1
Citrix Licensing Server	Windows Server 2008 R2	Lisenssipalvelin. Asennetaan tyypillisesti SQL-palvelimen yhteyteen.	1
Citrix Desktop Controller	Windows Server 2008 R2	Virtuaalityöpöytien hallintapalvelimet.	2
Web Interface -palvelin	Windows Server 2008 R2	Selainpohjaista pääsyä varten.	1
Citrix Merchandising Server	Vmware OVF-kuva.	Citrix Receiver –ohjelmiston jakelua ja päivitystä varten.	1
Netscaler VPX (Access Gateway)	Vmware OVF-kuva.	Etäkäyttöä varten. Linkitetään Web Interface –palvelimeen.	1
Isäntäkuva	Windows 7 -työasema	Isäntäkuva varsinaisia VDI työpöytiä varten.	1
VDI-työpöydät	Klooneja isäntäkuvasta.	Käyttäjäkohtaiset VDI työpöydät	10

Asennuksessa on hyvin monta vaihetta, jolloin ohjeita tulee noudattaa tarkoin ja järjestyksessä. Osan vaiheista voi jättää pois tietyissä tapauksissa, kuten esimerkiksi silloin, jos verkosta löytyy valmiina SQL-palvelin, jota voi käyttää. Asennusprosessissa on tärkeää seurata yrityksen omaa tietoturva- ja IT-politiikkaa erityisesti AD:n Group Policy määrittelyissä. Lisäksi lukuisia palvelimia asentaessa on oleellista varmistaa, että kaikki palvelimet ovat riittävän suojattuja erilaisia uhkia vastaan.

4 Aruba ClearPassin käyttöönotto

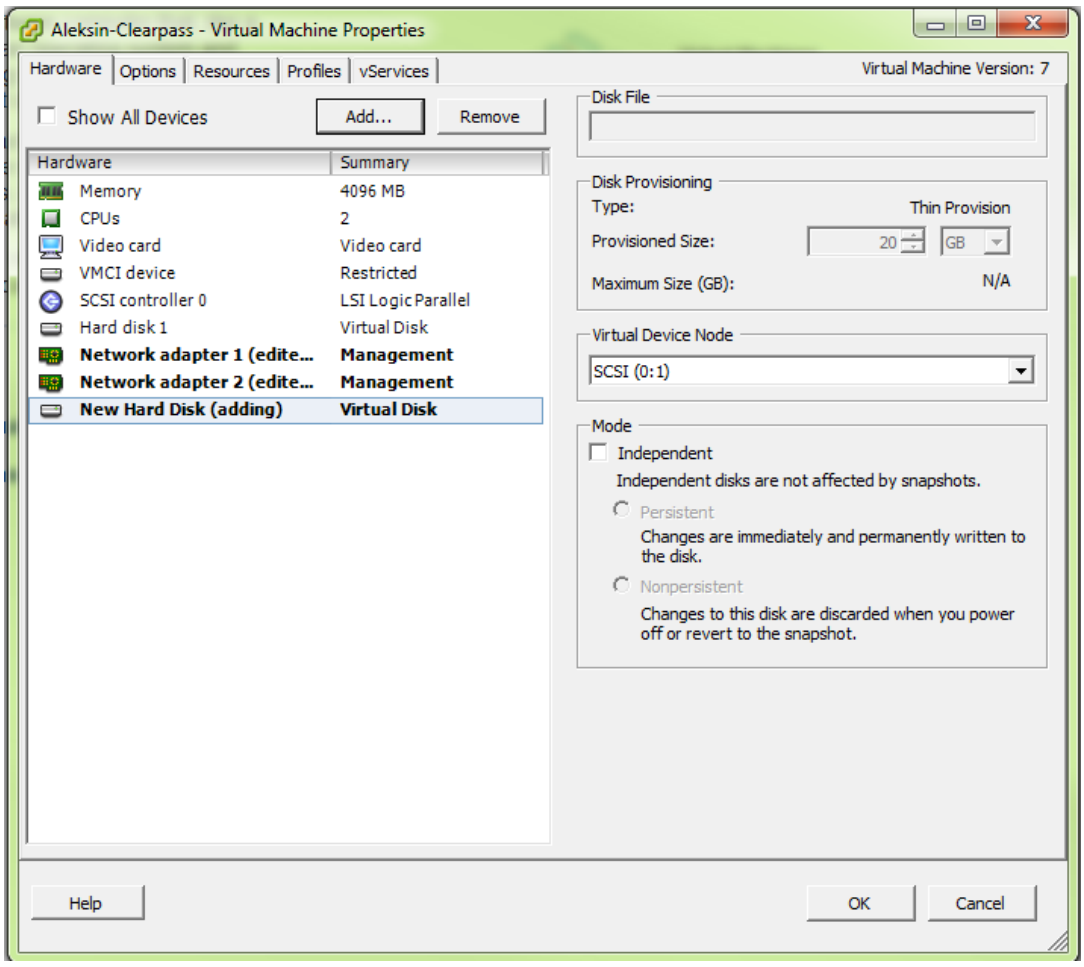
4.1 Asennus

Tässä osiossa asennetaan Aruba ClearPass Vmware-alustalle. Työn rajaamisen vuoksi ClearPass konfiguroidaan vain langattomaan verkkoon ja asennusvaiheessa oletetaan seuraavia asioita:

- Wmware-ympäristö on olemassa, siellä on riittävästi resursseja ja se on oikein konfiguroitu.
- Verkkoyhteydet ovat olemassa ja konfiguroitu esimerkiksi palomuurin osalta.
- Verkosta löytyy Aruban WLAN-kontrolleri verkkoasetukset konfiguroituna.
- Verkosta löytyy LDAP-palvelin konfiguroituna.

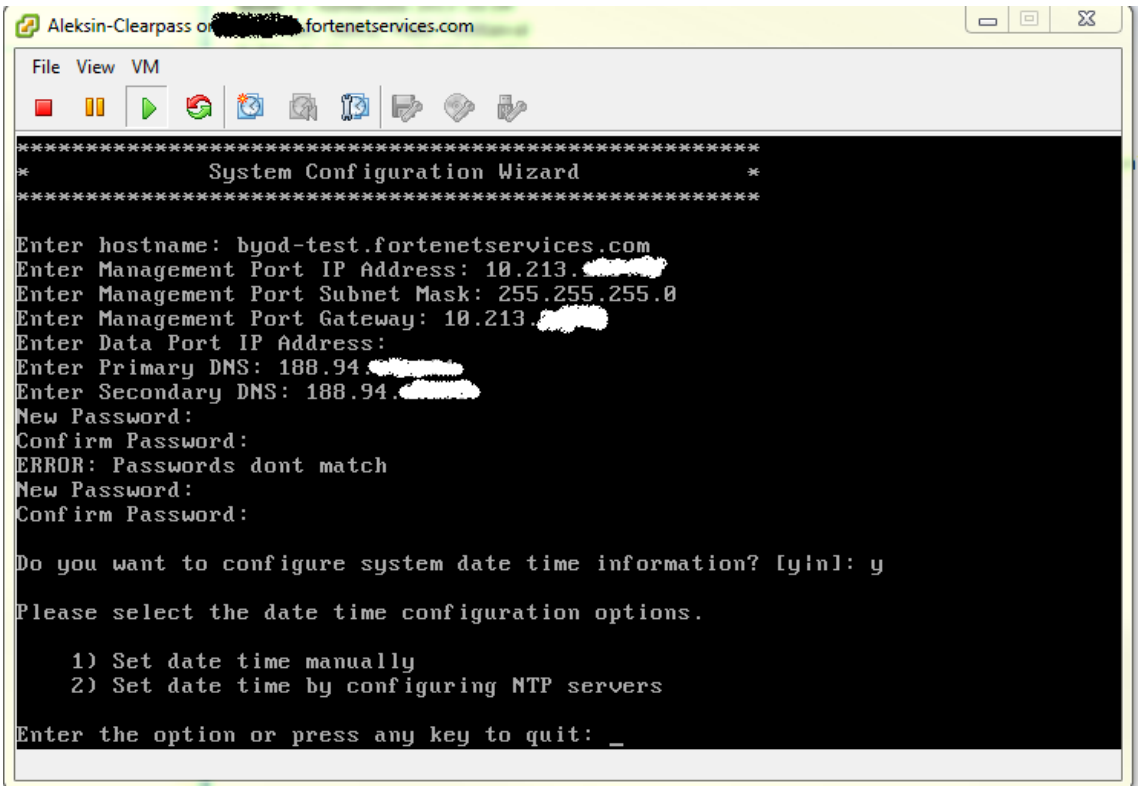
ClearPass Policy Managerin asennus alkaa lisenssien hankkimisesta. Arubalta on mahdollisuus hankkia 90-päivän kokeilulisenssi (evaluation), jolla voidaan asentaa kohta esiteltävä virtuaalinen kokeiluversio ClearPassista. Varsinainen lisenssi ostetaan suoraan Arubalta tai jälleenmyyjän kautta. Kokeilulisenssiä käyttäessä on syytä huomioida, että kokeilualustaa ei voi muuttaa maksulliseksi täysversioksi lisenssiä päivittämällä, vaan täysversio täytyy asentaa omana virtuaalikoneenaan. Kokeiluversiosta pystyy kuitenkin varmuuskopioimaan asetukset ja siirtämään ne laitteelta toiselle.

Lisenssien mukana tulee latauslinkki ja tunnukset, joiden avulla virtuaalisen ClearPassin voi ladata. Mukana on myös VM deployment guide, jonka ohjeita seuraamalla kokemattomampikin pystyy tekemään asennuksen. 1,6 gigatavun tiedosto on Vmwaren ymmärtämässä OVF-muodossa, joka tuodaan suoraan vSpheren kautta järjestelmään. Kokeilulaitteen tuominen kesti testiympäristössä noin 20 minuuttia. Kun OVF-kuvan tuominen on valmis, laitteelle lisätään yksi ylimääräinen kiintolevy ja varmistetaan, että verkkokortit ovat oikeassa verkossa ennen käynnistämistä. Ohjeissa ei mainittu, kuinka suuri levyn tulisi olla, niin testiin asennettiin 20 Gt thin-provisioned -levy.



Kuva 8. Ennen ensimmäistä käynnistystä ClearPassiin lisätään levy ja tarkastetaan, että verkkokortit ovat oikeassa verkossa.

Vmwareen asentamisen jälkeen uusi laite tulee sille määritetyllä nimellä näkyviin klusteriin, ja se voidaan käynnistää. Ensimmäisen käynnistyksen yhteydessä laite konfiguroi itse itsensä, jolloin käyttäjän tehtäväksi jää prosessin seuraaminen. Laite käynnistyy muutaman kerran uudestaan konfiguroidessaan itseään. Lopulta näkyviin tulee kirjautumisrivi, josta pääsee kirjautumaan tehdastunnuksella appadmin käyttäen salasanaa eTIPS123. Tämän jälkeen laitteeseen syötetään perusasetukset, kuten nimi, verkkoasetukset, uusi ylläpitäjän salasana ja kellonaika. ClearPassille on syytä tuotantoympäristössä määrittää kaksi IP-osoitetta, joista toinen on hallintaa ja toinen varsinaista dataa varten. Käytännöllisyyssyistä tässä työssä määritellään vain hallintaosoite. ClearPass siis voidaan tarvittaessa asettaa toimimaan myös yhdellä IP-osoitteella. Kun asetukset on tehty, laitteeseen voidaan yhdistää käyttäen määriteltyä IP-osoitetta tai mikäli laitteen IP on määritelty DNS-palvelimelle (suositeltavaa), niin DNS-nimeä. Tässä työssä laitteen DNS-nimeksi valittiin byod-test.



Kuva 9. Esiasetukset tehdään konsolissa.

Kun laitteeseen yhdistetään ensimmäisen kerran käyttäen https-protokollaa, tässä tapauksessa selaimella https://byod-test, laitteeseen lisätään lisenssit. Lisenssit löytyvät samasta sähköpostiviestistä, jossa oli latauslinkki. Ilman lisenssejä ja niiden aktivointia Policy Manageriin ei voi kirjautua sisään.

4.2 Konfigurointi

4.2.1 WLAN-kontrolleri

WLAN-kontrollerin asetusten teko on alustakohtainen, eikä siihen keskitytä paljoa tässä työssä, koska tutkimuksen kohteena on BYOD-järjestelmä. Tässä työssä ClearPassia käyttää Aruban WLAN-kontrolleri, johon on konfiguroitu kaksi SSID:tä: BYOD-auth ja BYOD. Auth-verkko on tarkoitettu laitteiden rekisteröintiä varten eikä siinä ole salausta. Auth-verkkoon liittyvät käyttäjät ohjataan Captive Portaliin, joka on ClearPass OnBoardin rekisteröintisivu https://<clearpass-ip>/guest/device_provisioning.php. Sivun nimen ja sisällön pystyy muuttamaan OnBoardin kautta Web Logins -asetussivulta. Todennus ja kirjautuminen tapahtuu ClearPassista RADIUS-protokollaa käyttäen. Käyttäjät saavat aluksi WLAN-kontrollerille konfiguroidun BYOD-auth -roolin ja

kirjautumisen sekä laitteen rekisteröimisen jälkeen varsinaisen BYOD-roolin. Auth-roolissa ei ole pääsyä muualle kuin rekisteröimissivulle. BYOD-roolissa pääsyä ei ole tässä työssä rajattu, vaan onnistuneesti laitteensa rekisteröinyt käyttäjä voi yhdistää minne vain.

Kuva 10. WLAN-kontrollerin roolit.

WLAN-kontrollerille konfiguroidaan seuraavassa taulukossa esitetyt asiat.

Taulukko 5. WLAN-kontrollerin määritykset.

Objekti	**Määritys**	**Kuvaus**
Roolit	Roolit BYOD-auth ja BYOD ja näiden palomuurisäännöt	Käyttäjän kulloinkin saaman roolin mukaan määräytyy kontrollerin antamat liikennöintoikeudet (ts. palomuuri).
Palvelimet	RADIUS ja RFC 3576 -palvelimet	Asetus kertoo kontrollerille tunnistautumistiedot yms. palvelimille, joista tietoa haetaan ja saadaan.
AAA-profiilit	AAA-BYOD ja AAA-BYOD-auth	AAA-profiiliin määritetään mistä todennus ja kirjautumistietoja tarkastetaan ja mistä valtuutus saadaan.
SSID-profiilit	BYOD ja BYOD-auth –SSID-profiilit	SSID-kohtaiset asetukset, kuten salaus, verkon nimi, jne.
L3-autentikointi, Captive Portal	BYOD Captive Portal -profiili	Profiili ensirekisteröintiin ohjausta varten.
Virtual AP-profiilit	VAP-BYOD ja VAP-BYOD-auth	Määrittää asetukset, mihin VLAN:in käyttäjä yhdistetään kulloinkin ja mitä AAA- sekä SSID-profiilia käytetään.
AP group	BYOD	Sisältää mm. VAP-profiilit, joiden mukaan määräytyy mitä verkkoja tukiasema mainostaa ja näiden verkkojen (yllä) asetukset. Tukiasema asetetaan käyttämään tätä AP grouppia.

Kontrollerin asetusten teon jälkeen tukiasema(t) asetetaan valmiiseen BYOD AP groupiin. Tämän jälkeen tukiasema hakee uudet asetukset kontrollerilta ja alkaa mainostaa asetusten mukaisia verkkoja (SSID). Kontrollerin, erityisesti Aruban, konfiguroiminen on erittäin monimutkaista, jos sitä ei ole koskaan aiemmin tehnyt. On suositeltavaa käyttää apuna riittäviä ohjeita asetusten oikein saamiseksi. Muiden valmistajien kontrollereilla asetukset ovat erilaisia, mutta perusajatus on kaikissa sama: Konfiguroidaan kaksi SSID:tä, joista toinen on rekisteröitymistä varten ja toinen varsinaista 802.1x BYOD:a varten. Kummassakin tapauksessa RADIUS-palvelimena toimii ClearPass, BYOD-auth verkossa tosin pelkän accountingin osalta. Koko järjestelmän voi rakentaa myös vain yhtä SSID:tä käyttäen. Yhteensopivuusongelmia esimerkiksi iOS 4 -laitteiden kanssa välttääkseen kannattaa konfiguroida kaksi erillistä verkkoa.

4.2.2 Palomuuri

Mikäli ClearPassin ja WLAN-kontrollerin välissä on palomuuri, täytyy palomuurilta avata vähintään seuraavat portit, jotta kontrolleri voi liikennöidä ClearPassiin:

- HTTPS (tcp/443)
- HTTP (tcp/80)
- RADIUS (tcp/1812, tcp/1813)
- RADIUS CoA (tcp/3799)
- ICMP

Luonnollisesti palomuurilta tulee myös tehdä avaukset WLAN-käyttäjille, jotka liikennöivät kontrollerin kautta, sekä tukiasemille, jotka hakevat mm. asetuksia kontrollerilta. Suuryrityksessä ClearPass-kirjautuminen ja valtuutus tapahtuvat todennäköisesti LDAP- tai AD-palvelimelta, jolloin ClearPassilla pitää olla pääsy ko. palvelimelle/palvelimille. LDAP portti on 389 ja LDAPS on 636.

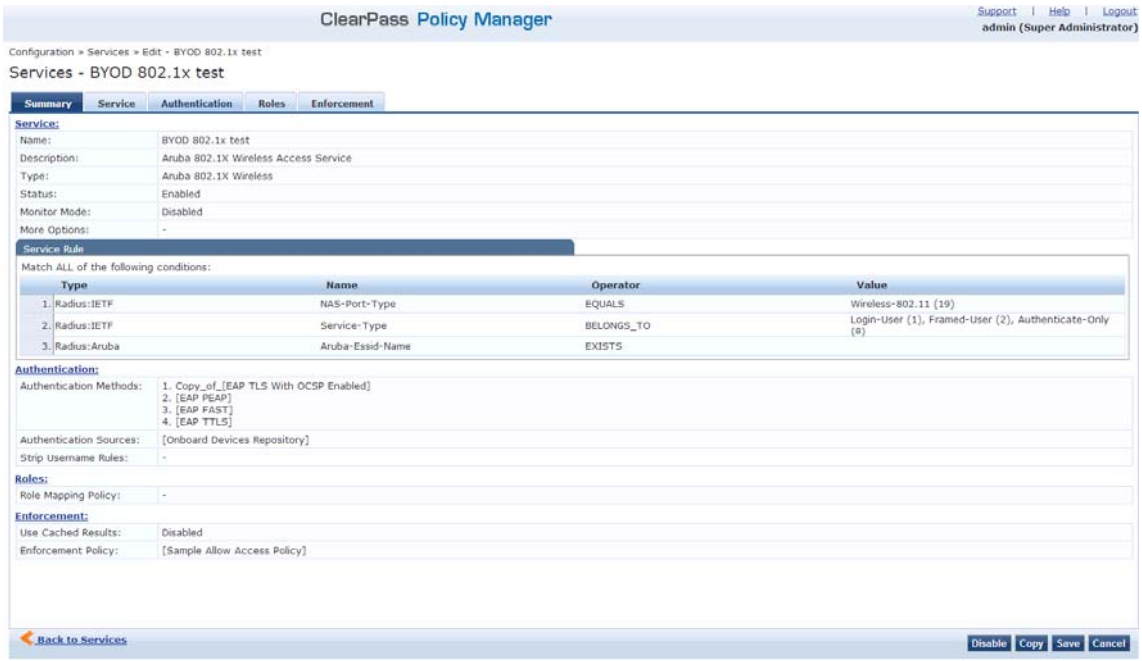
4.2.3 ClearPass PolicyManager

ClearPass Policy Manager toimitetaan useiden valmiiden oletusasetusten kanssa. Asetukset ovat pitkälti Amigopodin, Avendan ja Aruban yhteenliittämisen seurausta,

jonka vuoksi ne voivat vaikuttaa aluksi hyvin sekavilta. ClearPassin ulkoasu on kuitenkin selkeä, ja asetukset löytyvät nopeasti.

Policy Managerin käyttöönoton kannalta oleellisia osia ovat palvelut (services), kirjautumislähteet (authentication sources), roolit sekä vahvistuspolitiikat (enforcement policies) ja vahvistusprofiilit (enforcement profiles).

Konfigurointi alkaa configuration-sivulta, josta löytyy selkeä valikko-objekti ”start here”. Sivulta löytyy useita vaihtoehtoja, kuten Aruba 802.1x Wireless, 802.1x wireless, 802.1x wired, MAC authentication ja niin edelleen. Koska tässä työssä käytetään Aruban WLAN-kontrolleria, voidaan työssä käyttää mallinetta Aruba 802.1x wireless. Klikkaus aloittaa uuden palvelun luomisen. Palvelu pitää sisällään valmiiksi määritellyt palvelusäännöt, joita ei tarvitse muuttaa. Palvelulle annetaan kuvaava nimi, esimerkiksi tässä työssä *BYOD 802.1x test*. Suurin osa asetuksista voidaan jättää oletusasetuksille, kunhan varmistetaan, että kirjautumislähteeksi on valittu OnBoard Devices Repository. OnBoardin kautta rekisteröidyt laitteet lisätään automaattisesti kyseiseen SQL-tietokantaan. Enforcement-välilehdellä varmistetaan, että vahvistuspolitiikkana on *Sample Allow Access Policy*, jonka jälkeen uusi palvelu voidaan tallentaa.

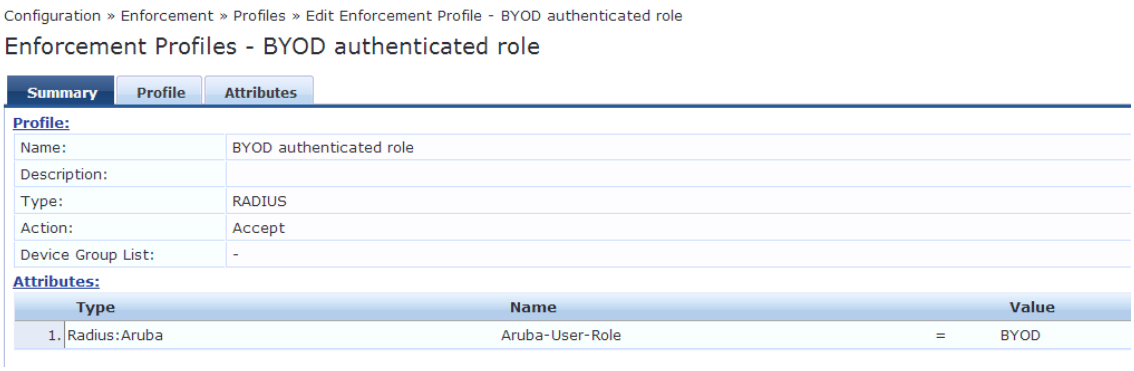


Kuva 11. Uuden 802.1x-palvelun yhteenvetosivu.

Uusi palvelu luodaan listan alimmaiseksi ja palveluiden järjestyksellä on hieman palomuurisääntöjen tavoin merkitystä. On suositeltavaa, ettei itse luotuja palveluita nosteta oletuksena luotujen palveluiden ylle, koska jokin toiminnallisuus voi siitä kärsiä. Tässä työssä vieraisiin liittyvät valmiit palvelut poistettiin käytöstä.

Jotta ClearPass pystyy tunnistamaan WLAN-kontrollerin, se täytyy lisätä järjestelmään. Configuration → Network → Devices -valikosta voidaan lisätä uusi tunnettu verkkolaite, joka tässä tapauksessa on WLAN-kontrolleri. Erityisen tärkeää on lisätä sama radiuksen jaettu avain ja mikäli mahdollista, niin valita laitetoimittajalistalta oikea laitetoimittaja.

Vahvistusprofiililla määritellään, mitä ClearPass palauttaa WLAN-kontrollerille RADIUS-kyselyyn. Vastaus voi olla esimerkiksi käyttäjän rooli tai VLAN. Usein profiileita luodaan useita, jotta WLAN-kontrollerilla voidaan ohjata tietyn ryhmän käyttäjät oikeaan rooliin. WLAN-kontrollerilla rooleihin on määritelty esimerkiksi pääsyoikeuksia. Rooleja voi olla esimerkiksi vieras, aliurakoitsija tai työntekijä. Tässä työssä käytetään yksinkertaistamiseksi vain yhtä roolia, ”BYOD”, joka on määritelty WLAN-kontrollerille. Kyseinen rooli antaa oletuksena pääsyoikeudet kaikkialle. Configuration → Enforcement → Profile valikosta luodaan uusi vahvistusprofiili, jonka nimeksi tässä työssä annettiin *BYOD authenticated role.* Profiilin mallinneeksi asetetaan Aruba RADIUS Enforcement. Profiilin asetuksista määritellään, onko vastaus RADIUS accept, reject vai drop ja valinnoissa voidaan vain muokata arvo (value) kohtaa, johon syötetään palautettavan roolin nimi, tässä tapauksessa BYOD. Mikäli tätä toimenpidettä ei tehdä, käyttäjät eivät voi liittyä varsinaiseen 802.1x-verkkoon.



Kuva 12. Uuden vahvistusprofiilin luominen on välttämätöntä, jotta kirjautuneet käyttäjät saavat oikeudet verkkoon. Kuvan attribuutteihin voidaan asettaa mm. VLAN.

Vahvistuspolitiikat ovat käytössä palveluissa ja niiden sisältö tulee vahvistusprofiileista. Äsken luotu vahvistusprofiili *BYOD authenticated role* otetaan käyttöön *Sample Allow Access Policyssä*, jonka sääntöihin uusi vahvistusprofiili lisätään Actions-kenttään. Asian selkiyttämiseksi yhteenveto koko kirjautumisprosessista ja siinä käytössä olevista komponenteista on esitetty graafisena luvun 4.2.4 lopussa.

ClearPass pystyy käyttämään muun muassa joko LDAP- tai AD-palvelinta käyttäjien tunnistamiseen. Palvelin lisätään Configuration → Authentication → Sources -valikon kautta. Tässä työssä käytettiin Open LDAP -palvelinta, jossa oli useita käyttäjätunnuksia valmiina. Mikäli kuitenkin käytetään AD-palvelinta, on syytä huomioida, että ClearPass täytyy liittää domainiin, jotta tietojen haku AD-palvelimelta varmasti onnistuu. ClearPass voidaan tarvittaessa myös liittää samanaikaisesti useaan domainiin. LDAP- tai AD-palvelimen voi ottaa käyttöön laitteelta valmiiksi löytyvässä *Onboard authorization* -palvelussa lisäämällä sen kirjautumislähteisiin tai sille voidaan luoda myös kokonaan uusi palvelu. Onboard authorization -palvelu tarkastaa, onko käyttäjällä oikeus rekisteröidä laitettaan ja samalla palvelulla sitä rajataan. Tässä työssä lisättiin LDAP:n lisäksi useita paikallisia käyttäjiä Configuration → Identity → Local Users -valikon kautta. Käyttäjillä simuloitiin eri laitteita, kuten esimerkiksi tunnuksella *test-win7* Windows 7 -tietokonetta.

ClearPass Policy Managerin osalta kriittisimpien asetusten teko on valmis. Administration → Agents and software update -valikon kautta on syytä käydä lisäämässä Subscription ID, jonka avulla ClearPass hakee ja päivittää automaattisesti tietokantojaan, kuten esimerkiksi laitteiden sormenjälkiä. Myös järjestelmäpäivitys voidaan tarvittaessa tehdä tämän valikon kautta.

4.2.4 ClearPass OnBoard

ClearPass OnBoard on Policy Managerin rinnalla ajettava sovellus, joka mahdollistaa laitteiden automaattisen rekisteröinnin ilman IT:n toimenpiteitä. IOS- ja uusimmille OS X -laitteille voidaan ladata OnBoardin kautta pelkkä sertifikaatti, mutta Windowsin ja Androidin osalta käytetään käyttäjätunnusta ja salasanaa.

OnBoard avataan Policy Managerin etusivulla olevasta linkistä tai siirtymällä https://<clearpass-ip>/tips -sivulle. Ensimmäisenä määritellään sertifikaattiasetukset, jotta ClearPass OnBoard jakaa oikeat sertifikaatit. Oletuksena OnBoard toimii

sertifikaattien juurimyöntäjänä (Root CA), mutta yleensä tuotantokäytössä se on asetettu toimimaan välillisenä (intermediate) myöntäjänä. Sertifikaattiasetuksissa määritellään tyypilliset asetukset ja joko tallennetaan uusi juurimyöntäjän sertifikaatti tai käydään allekirjoittamassa luotu sertifikaattipyyntö omalla tai esimerkiksi kaupallisella myöntäjällä.

Provisioning Settings -valikossa tehdään asetukset laitteiden rekisteröinnille. Sivulla määritetään muun muassa organisaation nimi, myönnettyjen laitesertifikaattien voimassaoloaika sekä kuinka monta laitetta kukin käyttäjä voi rekisteröidä omilla tunnuksillaan. Asetusten kautta tehdään myös valinnat alustakohtaisesti. IT voi esimerkiksi päättää, ettei Windows-laitteita voi rekisteröidä BYOD-laitteeksi yrityksen verkkoon. Samalla voidaan myös muokata laitekohtaisia rekisteröintisivuja ja niillä näkyviä ohjeita. OnBoard Client -välilehdellä on tärkeää huomata, käytetäänkö rekisteröintiin IP-osoitetta vai DNS-nimeä. Tämä riippuu siitä, miten WLAN-kontrollerin Captive Portal on määritetty ohjaamaan. Tässä työssä käytettiin IP-osoitetta. Lisäksi, koska työssä ei käytetty kaupallisen myöntäjän allekirjoittamaa sertifikaattia web-palvelimelle, täytyi web-palvelimen sertifikaatti jättää tarkistamatta. Jos web-palvelimella ei ole tunnetun myöntäjän allekirjoittamaa sertifikaattia ja kyseinen asetus on määritetty tarkastamaan se, laitteita ei voi rekisteröidä vaan rekisteröintiprosessi epäonnistuu sertifikaatin tarkastamisvirheestä johtuen. OnBoard Client -asetuksista voidaan lisäksi vaihtaa logo ja lisätä esimerkiksi Help Deskin osoite. Käyttäjien varsinaista rekisteröimissivua voidaan muokata melko vapaasti OnBoardin Configuration → Web Logins -valikon kautta, mutta asetuksista löytyy tärkeitä valintoja, kuten koko laiterekisteröimisen päälle tai pois laittaminen.

Kuva 13. OnBoardin Provisioning Settings -sivulla määritetellään alustakohtaisesti asetuksia.

OnBoardin viimeinen tärkeä asetus on Network Settings. Kyseiset asetukset määrittelevät varsinaiset rekisteröinnin yhteydessä Quick Connect -sovelluksen tekemät verkkoasetukset. Asetuksiin määritellään esimerkiksi SSID, johon liitytään,

sekä SSID:n muut asetukset. Asetuksista tehdään myös alustakohtaisia valintoja, kuten käytettävät protokollat.

Kun asetukset on tehty, voidaan laitteita rekisteröidä järjestelmään. Seuraavana on esitetty prosessikaaviona käyttäjän rekisteröinnissä olevat elementit.

Kuvio 2. Laitteen rekisteröintiprosessi.

Prosessissa tulee huomata, että Policy Managerin ja WLAN-kontrollerin roolit eivät välttämättä ole samoja, mikä saattaa aiheuttaa sekaannusta. ClearPass Policy Manager vaatii, että jokaisella käyttäjällä on rooli. Tässä työssä käytettiin pitkälti laitteella valmiina olevia rooleja. Paikallisille käyttäjille annettiin lisäksi erikseen TestRole-niminen rooli.

4.3 Käyttäjien yhdistäminen ja käyttöönotto

4.3.1 Windows 7

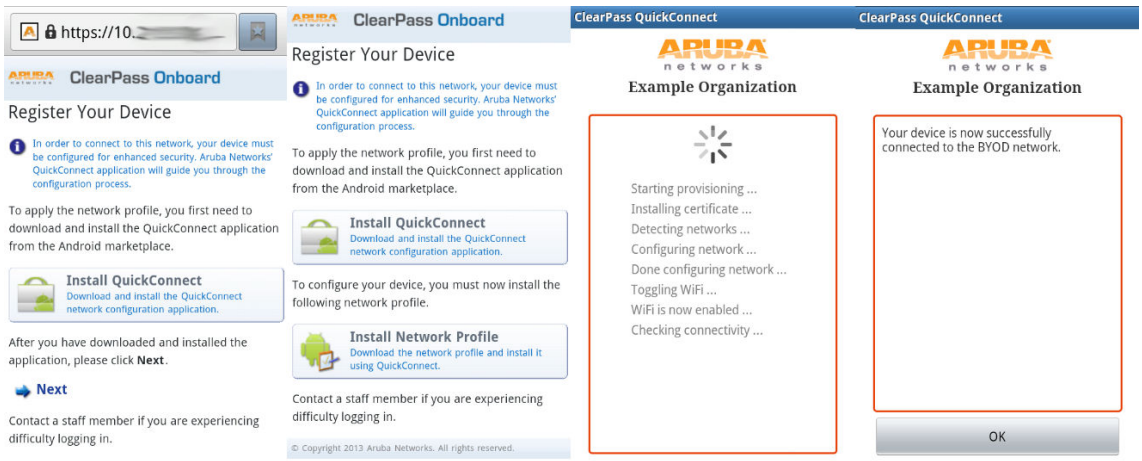
Työssä testattiin kahden erillisen Windows 7 -työaseman rekisteröimistä. Kummankin osalta prosessi oli Internet-selaimesta riippumatta sama, mutta toisella koneella käytettiin testimielessä LDAP-tunnusta ja toisella paikallista ClearPassiin luotua käyttäjätunnusta test-win7.

Testauksessa työasema yhdistettiin BYOD-auth -verkkoon, jolloin Windows ehdotti, että mahdollisia lisätietoja kirjautumisesta tarvitaan. Internet-selaimen avattua käyttäjä yhdistettiin portaaliin, josta ladattiin ja asennettiin QuickConnect-sovellus. Sovellukseen syötettiin käyttäjätunnus ja salasana, jonka jälkeen sovellus pyysi luvan asentaa tarvittavat sertifikaatit ja teki muut asetukset. Lopuksi sovellus ilmoitti asetusten olevan valmiit ja kehotti yhdistämään BYOD-verkkoon ohjelman connect-napilla. Tästä painamalla Windows vaihtoi 802.1x-verkkoon ja autentikoitui sujuvasti kysymättä tunnuksia.

Mikäli käyttäjällä ei ole ylläpitäjän oikeuksia tietokoneelle, hän ei voi rekisteröidä laitetta. QuickConnect vaatii ylläpitäjän tunnukset, jotka voi syöttää ohjelmaan, jos ohjelmaa ei suoriteta ylläpitäjän oikeuksilla.

4.3.2 Android

Android-laitteen rekisteröintiä testattiin sekä puhelimella että tabletilla. Android-laitteen rekisteröinnissä tuli vastaan myös ensimmäiset ongelmat. Kun laite yhdistettiin BYOD-auth-verkkoon, laite ohjattiin Windowsin tavoin rekisteröintiportaaliin selaimella. Androidin QuickConnect -sovellus ladataan kuitenkin Googlen Play-kaupasta, eikä suoraan ClearPassista, jolloin jos kauppaan pääsyä ei ole sallittu kirjautumattomille käyttäjille, ei käyttäjä pysty sovellusta lataamaan. Ongelman voi korjata lisäämällä kirjautumattomien käyttäjien rooliin WLAN-kontrollerille pääsyn android.clients.google.com ja *.ggpht.com -sivustoille. Ongelman voi myös kiertää asentamalla QuickConnect-sovelluksen etukäteen, mutta se ei ole käyttömukavuuden kannalta järkevää.



Kuva 14. Android-laitteen rekisteröinti.

Muilta osin Androidin rekisteröinti oli hyvin samankaltainen kuin Windowsinkin. Profiili ja sertifikaatti asennettiin juurikaan käyttäjän toimia tai osaamista vaatimatta ja WLAN SSID vaihdettiin asetusten teon jälkeen automaattisesti varsinaiseen 802.1x-verkkoon, johon laite myös tunnistautui onnistuneesti.

4.3.3 iPad

Applen laitteiden rekisteröinti tuotti melkoisia haasteita. Ensinnäkin täytyy varmistua siitä, että kaikki sertifikaatit (OnBoardin root ja signing sekä Policy Managerin webserver) ovat luotettuja. Lisäksi sertifikaatti täytyi vaihtaa siten, että se luodaan OnBoardissa laitteen sijasta, koska muuten laitetta ei jostain syystä lisätty Policy Managerin rekisteröityjen laitteiden listaan. Jotta iOS:lle etuna oleva pelkällä sertifikaatilla kirjautuminen onnistui, piti varmistaa, että EAP-TLS on käytössä Online Certificate Status Protocol (OCSP) valittuna. Tämä tarkoitti OCSP:n käyttöönottoa OnBoardissa, mikä on kuitenkin helppo toimenpide erityisesti, jos OnBoard toimii sertifikaattien juurimyöntäjänä.

Kuva 15. Access Tracker on erinomainen työkalu vikoja selvittäessä.

Kun iOS:n sertifikaatteihin liittyvät ongelmat saatiin ratkaistua, myös iPhone ja iPad rekisteröityivät ja verkkoa vaihtamalla tunnistautuivat 802.1x-verkkoon onnistuneesti.

4.3.4 Windows Mobile

Nokia Lumia 920 -puhelimella testatessa laite ohjautui oikein rekisteröintiportaaliin ja antoi mahdollisuuden ladata Windowsille suunnatun QuickConnect-sovelluksen. Ladatessa puhelin kuitenkin ilmoitti, ettei sovellus ole tuettu ja asennus keskeytyi. Valmistaja ei ole ilmoittanut Windows-puhelimien olevan tuettuja alustoja.

5 Tulokset

Sekä Citrixin että ClearPassin asennus vaatii aikaa ja perehtymistä järjestelmiin. Citrixin haasteena on asennusprosessin kesto, vaatimukset laajahkolle Windows-palvelinjärjestelmien tuntemiselle ja yhteenliittämishaasteet nykyisten järjestelmien kanssa. ClearPassin haasteena on monimutkainen roolien ja politiikkojen täyttämä järjestelmä, joka asentuu helposti ja nopeasti, mutta käyttöönotto voi olla aluksi haastavaa. Lisäksi ClearPassin asennus vaatii verkkolaitteiden, kuten WLAN-kontrollerin tuntemista sekä testailua. Mikäli ClearPassia käytetään myös langallisessa verkossa, täytyy käyttöönotossa varmistua, että kytkimet ja reitittimet tukevat 802.1x:ää.

Citrix on pitkän linjan toimija, jonka kehittämät järjestelmät ovat toimivia kokonaisuuksia ja käyttäjän näkökulmasta melko helppokäyttöisiä. Citrixin asennusprosessi on

kuitenkin hyvin monivaiheinen, ja vaikka esimerkiksi Internetistä on saatavilla useita asennusohjeita, on erinnäisiä asennushaasteita odotettavissa. Asennuksille kannattaakin varata riittävästi aikaa. Citrixin osalta myös lisensointi on melko vaikeaselkoinen, koska sekä järjestelmä ja käyttäjät että Windows-palvelimet täytyy lisensoida erikseen. Vmware-ympäristöltä vaaditaan Citrixin kohdalla paljon, koska virtuaalityöpöytien resurssit tulevat suoraan klusterin isäntäkoneilta.

Citrix on varma ratkaisu yritykselle, joka haluaa jatkaa niin kutsuttujen legacy-ohjelmistojen, kuten Microsoft Wordin käyttöä. Tietoturva on melko hyvä, koska tietoja ei tallennu käyttäjien päätelaitteisiin eikä päätelaitteilta ole suoraa pääsyä yrityksen järjestelmiin. Varmuuskopioiminen on helppoa, ja jos tiedot tallennetaan SAN:iin, eivät levyrikot kadota tietoja. Citrixin merkittävä ongelma on toimivuus kansainvälisessä yrityksessä, jossa työntekijät saattavat ottaa yhteyksiä VDI:hin pitkien etäisyyksien päästä. Järjestelmän luonne vaatii laadukkaan ja nopean yhteyden palvelimen ja käyttäjän välille, jolloin etäyhteyksillä tulevilla on usein käytön kanssa ongelmia. Toinen merkittävä ongelma on sovelluksien käytettävyys esimerkiksi kosketusnäyttölaitteella. Citrixin kautta pystytään jakelemaan ensisijaisesti vain Windowsia ja sen ohjelmia, joita ei ole suunniteltu käytettäväksi kosketuslaitteella, vaan hiirellä ja näppäimistöllä.

ClearPassin suurimpia haasteita on laitetuki, monen valmistajan laitteista koostuva tietoverkko sekä vaatimus tarkoin suunnitellulle pääsyn rajaukselle. Tässä työssä testattiin järjestelmää Aruban verkkolaitteilla, jolloin järjestelmän toimivuuden voidaan olettaa olevan parempi jo lähtökohtaisesti kuin esimerkiksi kokonaan toisen valmistajan WLAN-kontrollerin kanssa. ClearPass OnBoard ei myöskään tue Windows Mobile -alustaa, jolloin esimerkiksi Nokian puhelimia ei voida rekisteröidä itse. ClearPass saa jatkuvasti uusia ominaisuuksia ja päivityksiä, joiden kautta olettetavasti jossain vaiheessa tuki myös Windows Mobilen rekisteröimiselle saadaan.

Verkon rajauksen suunnittelu on tärkeä osa ClearPassin käyttöönottoa silloin, kun yritys tahtoo varmistaa hyvän tietoturvan. Järjestelmän käyttöönotto vaatiikin enemmän suunnittelutyötä kuin varsinaista asennustyötä. Asennustyö itsessään on nopea ja melko vaivaton prosessi. Syvä perehtyminen monimutkaisiin palvelu-rooli-käyttäjä-laite -kuvioihin on tarpeen, koska ClearPassiin on vielä melko vähän erilaisten ratkaisujen dokumentaatiota ja esimerkiksi OnBoardin käyttöönottoon ei valmista kohta kohdalta asennusohjetta löydy. Tutkimuksessa selvisi myös, että työssä käytetty auth-verkko voidaan melko helposti täydentää myös vierailijaverkoksi, jossa vierailijat voivat rekisteröityä itse. Toiminnallisuus kertookin siitä, että ClearPass skaalautuu hyvin

lukuisiin tutkimuksen ulkopuolelle jätettyihin toiminnallisuuksiin. Koska se on suunnattu laitevalmistajasta riippumattomaksi järjestelmäksi, houkuttelee se järjestelmän hankintaan, mutta järjestelmän valitsemista miettiessä tulee arvioida sen sopivuus yrityksen nykyiseen tietoverkkoon.

Perinteisessä toimistokäytössä Citrix XenDesktop on hyvä ja toimiva ratkaisu. Se ei kuitenkaan skaalaudu riittävässä määrin kansainvälisen yrityksen ja mobiilin työvoiman vaatimuksiin WAN-verkon haasteiden vuoksi. XenDesktop tuonee pitkällä aikavälillä yritykselle operatiivisista kustannuksista säästöjä, kun taas ClearPass todennäköisesti lisää IT:n kustannuksia. ClearPassin etuna on, että se on tuore ja nopeasti kehittyvä ratkaisu, jolla on selkeä tavoite laajentua toimimaan kokonaisvaltaisena BYOD-järjestelmänä kaikille alustoille. Se toimii hyvin ympäri maailmaa liikkuville työntekijöille ja tuomalla työntekijöille vapautta työvälineiden valinnassa se tuo IT:n lähemmäksi työntekijöitä, bisnekselle parempia tuloksia uusien SaaS sovellusten mahdollisuuksien kautta ja voi olla sitä kautta kannattava hankinta. Lisäksi ClearPass tunnisti testeissä käytetyt laitteet hyvin ja hankki niistä kattavat tiedot omaan tietokantaansa. Sekä XenDesktop että Clearpass vaativat valvontaa ja ylläpitoa, jolloin ainakaan XenDesktopin osalta IT:stä ei voida täysin luopua. ClearPass on BYOD:n ominaispiirteiden mukaisesti ulkoistettavissa oleva ratkaisu. Käyttöönotossa kumpaankin järjestelmään perehtyminen on tärkeää, jolloin suunnittelu ja toteutus voi muutenkin olla järkevää hankkia ulkopuoliselta palveluntarjoajalta. Hyvällä suunnittelulla ainakin ClearPass-ympäristöstä voidaan rakentaa melko staattinen ja vähän muutoksia vaativa.

Kansainvälisen suuryrityksen kannalta kummatkin järjestelmät ovat omalta osaltaan hyviä ratkaisuja. BYOD on kuitenkin selvästi tulevaisuutta ja SaaS-malliset palvelut lisääntynevät merkittävästi tulevaisuudessa. Mobiili työvoima painostaa yrityksiä siirtymään pois sijaintiperustaisista VLANeista ja miettimään vaihtoehtoisia ratkaisuja. Siksi suuryrityksen kannattaakin selvittää mahdollisuuksia BYOD:n käyttöönottoon. ClearPass on esimerkki toimivasta BYOD:n pääsynrajausjärjestelmästä, johon yritys voi itse määritellä omat ehtonsa.

6 Loppusanat

Tässä insinöörityössä tutkittiin kahta markkinoilla olevaa järjestelmää, joiden avulla kansainvälisen suuryrityksen työntekijät voivat ottaa omat laitteensa mukaan päivittäiseen työhön. Työn tavoitteina oli selvittää järjestelmien käytettävyyttä, käyttöönoton helppoutta ja tietoturvaa.

Työn tavoitteiden voidaan sanoa täyttyneen. Citrix XenDesktopin osalta selvitettiin kattavasti asennusprosessi Vmware-ympäristöön ja tutustuttiin sen käyttöönottoon sekä tietoturvaan. Internetistä ja haastattelun avulla kerätyn materiaalin perusteella selvitettiin tyypillisiä XenDesktopin käytettävyyteen liittyviä seikkoja. Aruban ClearPassin osalta järjestelmä asennettiin laboratorio-olosuhteisiin ja sen käyttöönotto testattiin käytännössä useilla eri laitealustoilla painottaen mobiililaitteisiin.

Tulevia tutkimuksia varten suosittelen keskittymään vain jompaankumpaan järjestelmistä ja kartoittamaan niiden sisältä löytyvien ominaisuuksien toimivuutta. XenDesktopin osalta tutkimusta kannattaisi tehdä WAN-verkon ongelmien tarkemmaksi määrittämiseksi ja yleisen toimivuuden testaamiseksi, kun käyttäjiä on satoja tai jopa tuhansia. ClearPass on uutuutensa vuoksi mielenkiintoinen tutkimuksen kohde ja sen lukuisia ominaisuuksia sekä tietoturvan toimivuutta olisi syytä testata tarkemmin. Myös ClearPassiin kesällä liitettävä Workspace MDM-sovellus on BYOD:n kannalta hyvä tutkimuskohde.

Lähteet

1 Gartner Says 821 Million Smart Devices Will Be Purchased Worldwide in 2012; Sales to Rise to 1.2 Billion in 2013. Verkkodokumentti. Gartner. <http://www.gartner.com/newsroom/id/2227215>. 6.11.2012. Luettu 11.3.2013.

2 Dobbie&Greco. 2012. BYOD: How and why? Verkkoseminaari. <http://www.zdnet.com/au/byod-how-and-why-7000004407/> 10.10.2012. Katsottu 11.3.2013.

3 Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems. Verkkodokumentti. Fortinet. <http://www.fortinet.com/press_releases/120619.html>. 19.6.2012. Luettu 11.3.2013.

4 Wireless LAN. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Wlan>. Luettu 12.3.2013.

5 GSM. 2013. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/GSM>. Luettu 12.3.2013.

6 IEEE 802.11g-2003. 2013.Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/802.11g>. Luettu 12.3.2013.

7 Nokia 9500 Communicator. 2013. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Nokia_9500>. Luettu 12.3.2013.

8 Rokka, Hannu. 2013. Toimitusjohtaja, Forte Netservices Oy, Helsinki. Haastattelu 12.4.2013.

9 Weldon, Kathryn. 2012. Bring Your Own Device: How to Protect Business Information and Empower Your Employees at the Same Time. Current Analysis. Heinäkuu 2012. Luettu 13.3.2013.

10 Kenney&Pon. 2011. Structuring the Smartphone Industry: Is the Mobile Internet OS Platform the Key? J Ind Compet Trade 11 sivut 239–261. 7.6.2011. Luettu 13.3.2013.

11 Maxwell, Kerry. 2013. Buzzword BYOD. Verkkodokumentti. <http://www.macmillandictionary.com/buzzword/entries/byod.html>. 2.1.2013. Luettu 13.3.2013.

12 Miller, Voas, Hurlburt . 2012. BYOD: Security and Privacy Considerations. IEEE Xplore. Syys-Loka 2012. Luettu 13.3.2013.

13 Bring your own device. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/BYOD>. Luettu 13.3.2013.

14 Aruba Clear Pass. 2013. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/products/clearpass/>. Luettu 14.3.2013.

15 Husso, Ismo. 2012. Eivätkö firman tarjoamat työvälineet kelpaa? Tuo sitten itse oma laitteesi (Osa 2). Verkkodokumentti. <http://www.sulava.com/2012/08/eivatko-firman-tarjoamat-tyovalineet-kelpaa-tuo-sitten-itse-oma-laitteesi-osa-2/>. 27.8.2012. Luettu 13.3.2013.

16 Husso, Ismo. 2012. Eivätkö firman tarjoamat työvälineet kelpaa? Tuo sitten itse oma laitteesi. Verkkodokumentti. <http://www.sulava.com/2012/05/eivatko-firman-tarjoamat-tyovalineet-kelpaa/>. 29.5.2012. Luettu 13.3.2013.

17 Mobile device management. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Mobile_device_management>. Luettu 14.3.2013.

18 King, Rachel. 2013. Aruba intros 'network-fluent' WorkSpace BYOD management platform. Verkkodokumentti. <http://www.zdnet.com/aruba-intros-network-fluent-workspace-byod-management-platform-7000013621/>. 10.4.2013. Luettu 20.4.2013.

19 Aruba Networks' MOVE Architecture Accelerates the Enterprise Access Network Mobility Revolution. 2011. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/news-releases/aruba-networks-move-architecture-accelerates-the-enterprise/>. 15.3.2011. Luettu 15.3.2013.

20 Aruba ClearPass Policy Manager Data Sheet. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/pdf/products/DS_ClearPass_PolicyManager.pdf>. Luettu 20.3.2013.

21 Rashid, Fahmida Y. 2011. Aruba Networks Acquires Avenda Systems to Enhance BYOD Security Portfolio. Verkkodokumentti. <http://www.eweek.com/c/a/Security/Aruba-Networks-Acquires-Avenda-Systems-to-Enhance-BYOD-Security-Portfolio-389292>. 18.11.2011. Luettu 11.4.2013.

22 Aruba ClearPass FAQ. Verkkodokumentti. Aruba Networks. <http://www.mayflex.com/_assets/downloads/ClearPass_FAQ.pdf>. Luettu 23.3.2013.

23 Aruba MOVE White Paper. 2012. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/pdf/technology/whitepapers/WP_MOVE.pdf>. Luettu 11.4.2013.

24 Aruba ClearPass Policy Manager Deployment Guide. Laitedokumentaatio. Aruba Networks. Luettu 20.2.2013.

25 Aruba ClearPass OnGuard Data Sheet. 2012. Verkkodokumentti. Aruba Networks. <http://www.arubanetworks.com/pdf/products/DS_ClearPass_OnGuard.pdf>. Luettu 22.3.2013.

26 Aruba ClearPass OnBoard Deployment Guide. Laitedokumentaatio. Aruba Networks. Luettu 20.4.2013.

27 Mooren Laki. 2013. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Mooren_laki>. Luettu 23.3.2013.

28 What is Virtualization? Verkkodokumentti. Vmware. <http://www.vmware.com/virtualization/what-is-virtualization.html>. Luettu 23.3.2013.

29 Virtualization. 2013. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Virtualization>. Luettu 23.3.2013.

30 Desktop Virtualization For All. 2012. Dokumentaatio. Citrix. Luettu 23.3.2013.

31 Citrix XenDesktop DataSheet. 2012. Verkkodokumentti. Citrix. <http://www.citrix.com/content/dam/citrix/en_us/documents/solutions/datasheetxendesktop.pdf>. Luettu 3.4.2013.

32 Wolf, Chris. 2012. Desktop Virtualization Trends at Gartner Data Center. Verkkodokumentti. <http://blogs.gartner.com/chris-wolf/2012/12/10/desktop-virtualization-trends-at-gartner-data-center/>. 10.12.2012. Luettu 26.3.2013.

33 Jennings, Cath. 2009. VMware: five biggest challenges of server virtualisation. Verkkodokumentti. Computer Weekly. <http://www.computerweekly.com/feature/VMware-five-biggest-challenges-of-server-virtualisation>. Lokakuu 2009. Luettu 11.4.2013.

34 Bittman, Weiss, Margevicius, Dawson. 2012. Magic Quadrant for x86 Server Virtualization Infrastructure. Verkkodokumentti. Gartner. <http://www.gartner.com/technology/reprints.do?id=1-1B2IRYF&ct=120626&st=sg>. 11.6.2012. Luettu 26.3.2013.

35 Citrix XenDesktop Licencing. 2013. Verkkodokumentti. Citrix. <http://www.citrix.com/products/xendesktop/how-it-works/licensing.html>. Luettu 6.4.2013.

36 Citrix XenDesktop Editions. 2013. Verkkodokumentti. Citrix. <http://www.citrix.com/products/xendesktop/features/editions.html>. Luettu 6.4.2013.

37 Meesters, Rich. 2012. XenDesktop Planning Guide – vSphere. Verkkodokumentti. Citrix. <http://support.citrix.com/article/CTX132166>. 10.3.2012. Luettu 7.4.2013.

38 Citrix XenDesktop lisenssien hinnasto. 2013. Verkkodokumentti. Moonsoft verkkokauppa. <http://www.moonsoft.fi/products/000669.aspx>. Luettu 6.4.2013.

39 Meesters, Rich. 2011. XenDesktop Implementation Guide with vSphere 5. Verkkodokumentti. Citrix. <http://support.citrix.com/article/CTX131969>. 16.12.2011. Luettu 2.4.2013.